ANNALES DE L'INSTITUT FOURIER

MOHAMED AYAD

Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques

Annales de l'institut Fourier, tome 43, nº 3 (1993), p. 585-618
<http://www.numdam.org/item?id=AIF_1993__43_3_585_0>

Ann. Inst. Fourier, Grenoble
43, 3 (1993), 585–618

PÉRIODICITÉ (mod q) DES SUITES ELLIPTIQUES ET POINTS S-ENTIERS SUR LES COURBES ELLIPTIQUES

par Mohamed AYAD

1. Introduction.

Soit E une courbe elliptique définie sur $\mathbb{Q}$ par un modèle de Weierstrass généralisé :

$$(1.1) \qquad y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6, \qquad A_i \in \mathbb{Z}.$$

Soit $M \in E(\mathbb{Q})$. Pour tout entier $m \in \mathbb{Z}$, les coordonnées de mM s'expriment sous la forme :

$$mM = \left(\frac{\phi_m(M)}{\Psi_m^2(m)}, \frac{\omega_m(M)}{\Psi_m^3(M)}\right)$$

où ϕ_m, Ψ_m, ω_m sont des polynômes définis par récurrence [1]. Les formules utiles pour la suite sont rappelées dans le paragraphe 3. On pose :

$$\widehat{\Psi}_m = d^{m^2-1}\Psi_m(M), \quad \widehat{\phi}_m = d^{2m^2}\phi_m(M), \quad \widehat{\omega}_m = d^{3m^2}\omega_m(M),$$

de sorte que ces nombres sont des entiers. On notera que d'après 3.6, on a : $\widehat{\Psi}_m$ divise $\widehat{\Psi}_n$ si m divise n.

Le but du présent travail est d'étudier la périodicité (mod q) de la suite $(\widehat{\Psi}_m)$ lorsque M (mod p) est non singulier pour tout diviseur premier p de q. Nous examinons plus particulièrement la relation entre la période (mod p^e) et la période (mod p^{e+1}).

Mots-clés : Suites elliptiques – Points S-entiers – Courbes elliptiques – Périodicité (mod q).
Classification A.M.S. : 11B50 – 11B83 – 11D25 – 11G05.

Le problème de périodicité a été étudié pour les suites récurrentes linéaires [3], [5], [6], [10], [11], ainsi que pour les suites de convergents des développements en fractions continues des nombres réels dont le développement est purement périodique [2].

M. Ward a déjà étudié la périodicité (mod p) des suites elliptiques, lorsque p est un nombre premier. L'auteur a utilisé ici une méthode de démonstration différente de celle de Ward parce que la méthode de celui-ci ne paraît pas généralisable au cas de p^n. L'auteur a cherché en vain à comprendre l'allusion de Ward contenue dans la note en bas de la page 46 affirmant que « la périodicité pour un module arbitraire est une conséquence facile [10]. »

Les résultats obtenus sur la périodicité peuvent être utilisés pour la recherche des points S-entiers sur les courbes elliptiques de rang 1 sur $\mathbb{Q}$, comme nous le ferons complètement pour les courbes d'équations respectives $y^2 = x^3 - 13$ et $y^2 = x^3 + 40$ avec $S = \{2, 3, 5, 7\}$.

2. Énoncés des principaux résultats.

Avant de revenir au problème de la périodicité, reprenons le résultat suivant [1] : soient K un corps, E une courbe elliptique définie sur K par un modèle de Weierstrass généralisé :

$$y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6, \qquad A_i \in K. \tag{2.1}$$

Soit ν une valuation discrète sur K telle que $\nu(Ai) \geq 0$, alors on a le :

THÉORÈME A. — *Soit $M \in E(K)$ tel que $M \neq \infty$. On suppose que M (mod ν) $\neq \infty$. On pose :*

$$mM = \left(\frac{\phi_m(M)}{\Psi_m^2(M)}, \frac{\omega_m(M)}{\Psi_m^3(M)}\right).$$

Les propriétés suivantes sont équivalentes :

(a) $\nu(\Psi_2(M))$ *et* $\nu(\Psi_3(M)) > 0$.

(b) *Pour tout entier* $m \geq 2$, *on a* $\nu(\Psi_m(M)) > 0$.

(c) *Il existe un entier* $m_0 \geq 2$ *tel que* $\nu(\Psi_{m_0}(M))$ *et* $\nu(\Psi_{m_{0+1}}(M)) > 0$.

(d) *Il existe un entier* $n_0 \geq 2$ *tel que* $\nu(\Psi_{n_0}(M))$ *et* $(\phi_{n_0}(M)) > 0$.

(e) M (mod ν) *est singulier.*

On suppose dorénavant que $K = \mathbb{Q}$ et que $A_i \in \mathbb{Z}$; le modèle (2.1) étant quelconque pas nécessairement minimal.

Soit $M = (x, y) = (a/d^2, b/d^3)$ avec $(a, d) = 1$ un point de $E(\mathbb{Q})$. Pour tout entier m, on pose

$$mM = \Big(\frac{\phi_m(M)}{\Psi_m^2(M)}, \frac{\omega_m(M)}{\Psi_m^3(M)}\Big) = \Big(\frac{\widehat{\phi}_m}{d^2\widehat{\Psi}_m^2}, \frac{\widehat{\omega}_m}{d^3\widehat{\Psi}_m^3}\Big)$$

avec

$$\widehat{\phi}_m = d^{2m^2}\phi_m(M), \quad \widehat{\Psi}_m = d^{m^2-1}\Psi_m(M), \quad \widehat{\omega}_m = d^{3m^2}\omega_m(M).$$

Ces nombres $\widehat{\phi}_m$, $\widehat{\Psi}_m$, $\widehat{\omega}_m$ sont des entiers. Nous aurons recours au lemme suivant [1].

LEMME A. — *Soient S un ensemble fini de nombres premiers (éventuellement vide), $m \neq 0$ un entier rationnel et M un point rationnel de* (2.1) *d'ordre infini. Si mM est S entier, alors M est S entier.*

En d'autres termes, cela signifie que les nombres premiers qui divisent d ne se simplifient pas dans la dernière représentation de mM ($m \in \mathbb{Z}$) ci-dessus. Les nombres premiers qui peuvent se simplifier dans cette représentation sont caractérisés par le théorème A : ce sont les nombres premiers p de mauvaise réduction tels que M (mod p) est singulier. Le théorème A admet comme conséquence le résultat suivant [1].

COROLLAIRE A. — *Soient M un point rationnel d'ordre infini de* (2.1), *S un ensemble fini de nombres premiers contenant l'ensemble T* (*éventuellement vide*), *des nombres premiers p de mauvaise réduction tels que M* (mod p) *est singulier. Soit $m \in \mathbb{Z}$, $m \neq 0$. On suppose que M est S-entier. Pour que mM soit S-entier, il faut et il suffit que*

$$\widehat{\Psi}_m = \pm \prod_{p \in S} p^{e_p}$$

avec e_p entier ≥ 1 si $p \in T$ et entier ≥ 0 si $p \in S - T$.

Soient maintenant M un point rationnel d'ordre infini de (2.1) et p un nombre premier fixé tel que M (mod p) est non singulier. Le théorème A montre que p ne divise pas deux termes consécutifs de la suite d'entiers $(\widehat{\Psi}_m)$. Soit r l'ordre d'apparition de p dans la suite $(\widehat{\Psi}_m)$, c'est-à-dire le plus petit entier $m > 1$ tel que p divise $\widehat{\Psi}_m$.

• Si p divise d, le travail de Lutz [7] montre que $r = p$; on en donnera une preuve simple dans le paragraphe 3.

• Si p ne divise pas d, alors $M \pmod p \neq \infty$ et r = ordre de M dans $E(\mathbb{F}_p)_{n.s}$ Soit $e_0 = \nu_p(\widehat{\Psi}_r)$ avec $e_0 \geq 1$. On se réfèrera très souvent à cet exposant. Le théorème suivant caractérise l'ordre d'apparition de p^e dans la suite $(\widehat{\Psi}_m)$.

THÉORÈME B.

(i) *Soit r_e l'ordre d'apparition de p^e (où $e \geq 1$) dans la suite $(\widehat{\Psi}_m)$. Alors on a :*

$$r_e = \begin{cases} r & \text{si } e \leq e_0, \\ p^{e-e_0} \cdot r & \text{si } e > e_0. \end{cases}$$

(ii) *Plus précisément, pour tout $m \neq 0$, écrivons $m = r^{h_0} p^{h_1} n$ avec $h_1 \geq 0$, $(p, n) = 1$ et $h_0 = 0$ si $r \nmid m$ et $h_0 = 1$ si $r \mid m$. Alors on a :*

$$\nu_p(\widehat{\Psi}_m) = 0 \qquad \text{si} \quad h_0 = 0,$$

$$\nu_p(\widehat{\psi}_m) = h_1 + \nu_p(\widehat{\Psi}_r) = h_1 + e_0 \quad \text{si} \quad h_0 = 1.$$

Preuve. — Voir le paragraphe 3. (Ce résultat a été déjà démontré par Ward par une méthode quelque peu différente et sous des conditions plus restrictives [13].)

Ce théorème a pour conséquence immédiate que si $(\widehat{\Psi}_m)$ est périodique $\pmod{p^e}$ et si π_e est une période, alors r_e divise π_e. De son côté, la preuve de la périodicité $\pmod{p^e}$ de la suite $(\widehat{\Psi}_m)$ lorsque p est impair et $r \geq 3$ sera déduite du résultat suivant.

THÉORÈME C. — *Soient M un point rationnel d'ordre infini de* (2.1) *et p un nombre premier impair tel que $M \pmod p$ est non singulier. Soient r l'ordre d'apparition de p dans la suite $(\widehat{\Psi}_m)$ et r_e celui de p^e pour tout $e \geq 1$. On suppose que $r \geq 3$. Pour tout $(n, k) \in \mathbb{Z} \times \mathbb{Z}$, on a*

$$\widehat{\Psi}_{kr_e+n} \equiv a_e^{kn} b_e^{k^2} \widehat{\Psi}_n \pmod{p^e} \tag{2.2}$$

avec $a_e = \widehat{\Psi}_{r_e+2}/\widehat{\Psi}_2\widehat{\Psi}_{r_e+1}$ *et* $b_e = \widehat{\Psi}_{r_e+1}^2\widehat{\Psi}_2/\widehat{\Psi}_{r_e+2}$.

Preuve. — Voir le paragraphe 4.

En particulier, pour $k = 1$ et $n = 0, 1, \ldots, r_e$, on a :

$$\widehat{\Psi}_{r_e - n} \equiv a_e^{-n} b_e \widehat{\Psi}_{-n} \equiv -a_e^{-n} b_e \widehat{\Psi}_n \pmod{p^e}.$$

Nous dirons à la suite de Ward qu'il y a une certaine symétrie dans la distribution $(\mathrm{mod}\, p^e)$ des $r_e + 1$ premiers termes de $(\widehat{\Psi}_m)$. Avant d'énoncer le théorème suivant — qui est une conséquence du théorème C — adoptons les notations suivantes :

- Pour tout entier $e \geq 1$, on note $(\mathbb{Z}/p^e\mathbb{Z})^*$ le groupe des unités de $\mathbb{Z}/p^e\mathbb{Z}$.
- Pour tout $u \in \mathbb{Z}$, $(u, p) = 1$, on note $\theta_e(u)$ l'ordre de u dans le groupe $(\mathbb{Z}/p^e\mathbb{Z})^*$.
- L'expression « la période de $(\widehat{\Psi}_m)$ » désignera toujours dans le texte la plus petite période de $(\widehat{\Psi}_m)$. En fait, si π_e est la période de $(\widehat{\Psi}_m)$ mod p^e et si η_e est une période de $(\widehat{\Psi}_m)$ $(\mathrm{mod}\, p^e)$ alors π_e divise η_e.

Avec les notations précédentes et sous les hypothèses du théorème C, nous avons le :

THÉORÈME D. — *Soit k_e le plus petit entier > 0 tel que :*

$$a_e^{k_e} \equiv 1 \pmod{p^e} \quad et \quad b_e^{k_e^2} \equiv \pmod{p^e}. \tag{2.3}$$

Alors la suite $(\widehat{\Psi}_m)$ est périodique $(\mathrm{mod}\ p^e)$ et sa période π_e vérifie $\pi_e = k_e r_e$. De plus, $k_e = \theta_e(a_e)$ ou $k_e = 2\,\theta_e(a_e)$ et on a $k_e = 2\,\theta_e(a_e)$ si et seulement si $\theta_e(a_e)$ est impair et $\theta_e(b_e)$ est pair.

Preuve. — Voir le paragraphe 4.

On verra aussi dans ce paragraphe une méthode de calcul de la période $(\mathrm{mod}\, p^e)$ qui n'utilise pas l'ordre des éléments dans $(\mathbb{Z}/p^e\mathbb{Z})^*$.

Nous sommes maintenant en mesure d'énoncer le résultat, établissant la relation entre π_e et π_{e+1}, qui est notre objectif principal dans ce travail. Nous verrons dans le paragraphe 6 comment cette relation peut être utilisée pour la recherche des points S-entiers sur les courbes elliptiques de rang 1 sur $\mathbb{Q}$.

THÉORÈME E. — *Soient M un point rationnel d'ordre infini de* (2.1), *p un nombre premier impair tel que M $(\mathrm{mod}\ p)$ est non singulier et r l'ordre d'apparition de p dans la suite $(\widehat{\Psi}_m)$. Soient $a_1 = \widehat{\Psi}_{r+2}/\widehat{\Psi}_2\widehat{\Psi}_{r+1}$ et $\theta_1 = \theta_1(a_1)$. Soient $e_0 = \nu_p(\widehat{\Psi}_r)$, $e_2 = \nu_p(a_1^{\theta_1} - 1)$ et $e_1 = \inf(e_0, e_2)$. Alors on a $\pi_1 = \cdots = \pi_{e_1}$ et $\pi_e = p^{e-e_1}\pi_1$ pour $e > e_1$.*

Preuve. — Voir le paragraphe 5.

Ce théorème signifie que la période (mod p^e) est stationnaire jusqu'à un certain rang $e_1 \leq e_0$, effectivement calculable et qu'à partir de ce rang on a : $\pi_{e+1} = p\pi e$. En particulier si $e_0 = 1$ alors $e_1 = e_0 = 1$.

Dans les deux exemples qui suivent on a $p = 5$, $e_0 = 2$, $e_1 = 1$ dans le premier cas et $p = 5$, $e_0 = 2$, $e_1 = 2$ dans le second.

Exemple 1 : $y^2 = x^3 - x - 5$ et $M = (2, 1)$.

On a $r = r(5) = 4$, $\nu_5(\widehat{\Psi}_4) = 2$, $e_0 = 2$, $e_1 = 1$, $\pi_1 = \pi(5) = 16$ et $\pi_e = 5^{e-1}\pi(5) = 5^{e-1} \cdot 16$ pour $e \geq 2$.

Exemple 2 : $y^2 = x^3 - 15x$ et $M = (4, 2)$.

On a $r = r(5) = 5$, $\nu_5(\widehat{\Psi}_5) = 2$, $e_0 = 2$, $e_1 = 2$, $\pi_1 = \pi_2 = 10$ et $\pi_e = 5^{e-2}\pi_1 = 2 \cdot 5^{e-1}$ pour $e \geq 3$.

On observera que — dans les théorèmes C, D, E — l'on a supposé que $p \neq 2$ et $r \geq 3$. L'auteur espère traiter ultérieurement les cas $p = 2$, $r \geq 3$ et p quelconque, $r = 2$. Comme conséquence du théorème précédent nous obtenons le :

THÉORÈME F. — *Soient $M = (a/d^2, b/d^3)$ un point rationnel de* (2.1) *et p un nombre premier impair tel que M* (mod p) *est non singulier. On suppose que $\nu_p(\widehat{\Psi}_p) = 1$, $\widehat{\Psi}_{p-1}\widehat{\Psi}_{p+1} \equiv -1$* (mod p^2) *et $\pi_1 = p$. On suppose aussi que les éléments $\widehat{\Psi}_m$ ($1 \leq m \leq p^2 - 1$ premier à p), sont distincts deux à deux* (mod p^2). *Alors on a :*

1) *La suite $(\widehat{\Psi}_m)$ est périodique* (mod p^N) *et sa période vérifie $\Pi_N = p^N$ pour tout entier $N \geq 1$.*

2) *Pour tout entier $N \geq 2$,*

$$\widehat{\Psi}_{p^{N-1}-1}\widehat{\Psi}_{p^{N-1}+1} \equiv -1 (\mathrm{mod}\, p^N). \tag{2.4}$$

3) *Les entiers $\widehat{\Psi}_m$ ($1 \leq m \leq p^{N-1}$ premiers à p) sont distincts deux à deux* (mod p^N) *pour tout entier $N \geq 1$.*

4) *$\widehat{\Psi}_m = \pm 1$ si et seulement si $m = \pm 1$.*

Preuve. — Voir le paragraphe 6.

Comme conséquence immédiate de ce théorème et à la lumière du corollaire A et de la propriété de l'ordre d'apparition des nombres premiers, dans les suites elliptiques (voir commentaire précédent le théorème B), on déduit que si M vérifie les hypothèses du théorème F et si de plus M (mod ℓ) est non singulier pour tout nombre premier ℓ de mauvaise réduction et si on prend pour S l'ensemble des diviseurs premiers de d alors :

$$mM \ S\text{-entier} \implies m = \pm p_1^{e_1} \cdots p_s^{e_s},$$

où $p_i \in S$ et où les $e_1, \ldots, e_s$ sont des entiers ≥ 0.

Dans le paragraphe 6, nous traiterons complétement les points S-entiers sur les courbes d'équation respectives $y^2 = x^3 - 13$ et $y^2 = x^3 + 40$ avec $S = \{2, 3, 5, 7\}$.

Nous traiterons aussi le cas des multiples S-entiers du point $M = \big(1/5^2, (1+5k)/5^3\big)$ sur la courbe $y^2 = x^3 + 2kx + 25k^2$ lorsque $S = \{5\}$ et k entier $\neq 0$, $(k, 5) = 1$.

3. Rang d'apparition de p^e.

Rappelons d'abord les formules donnant $\phi_m(M), \Psi_m(M), \omega_m(M)$ valables sur un corps quelconque. On omettra M dans ces formules sauf dans (3.6).

$$\begin{aligned}
\Psi_0 &= 0,\\
\Psi_1 &= 1,\\
\Psi_2 &= 2y + A_1 x + A_3,\\
\Psi_3 &= 3x^4 + B_2 x^3 + 3B_4 x^2 + 3B_6 x + B_8\\
\Psi_4 &= \Psi_2\Big[2x^6 + B_2 x^5 + 5B_4 x^4 + 10B_6 x^3 + 10B_8 x^2\\
&\qquad\qquad + (B_2B_8 - B_4B_6)x + (B_4B_8 - B_6^2)\Big]
\end{aligned}$$

où les B_i sont les polynômes classiques en les A_i.

$$\Psi_2\Psi_{2m} = \Psi_m(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2), \tag{3.1}$$

$$\Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3, \tag{3.2}$$

$$\Psi_m = -\Psi_{-m}, \tag{3.3}$$

$$(3.4)\quad \begin{cases} \phi_m = x\Psi_m^2 - \Psi_{m-1}\Psi_{m+1}, \\ \omega_m = \dfrac{\Psi_{2m}}{2\Psi_m} - \frac{1}{2}\Psi_m(A_1\phi_m + A_3\Psi_m^2), \end{cases}$$

$$(3.5)\qquad \Psi_{u+v}\Psi_{u-v} = \Psi_{u+1}\Psi_{u-1}\Psi_v^2 - \Psi_{v+1}\Psi_{v-1}\Psi_u^2 \quad (u, v \in \mathbb{Z}),$$

$$(3.6)\qquad \Psi_{mn}(M) = \Psi_n^{m^2}(M)\Psi_m(nM),$$

$$\Psi_m \in \mathbb{Z}[A_1, \ldots, A_6, x] \quad \text{si } m \text{ est impair},$$

$$\Psi_m/(2y + A_1x + A_3) \in \mathbb{Z}[A_1, \ldots, A_6, x] \quad \text{si } m \text{ pair}.$$

Cela étant, soit M un point rationnel d'ordre infini sur la courbe :

$$(3.7)\qquad y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6, \qquad A_i \in \mathbb{Z}.$$

Soit p un nombre premier tel que $M(\text{mod } p)$ est non singulier (ce qui est toujours vérifié si p divise d).

Le lemme qui suit a déjà été démontré dans [7] lorsque la courbe est définie sur un corps $\mathfrak{p}$-adique $K_{\mathfrak{p}}$ mais avec un modèle de Weierstrass court.

Lemme 1. — *Soit* $M = (a/d^2, b/d^3)$, *avec* $(a, d) = 1$, *un point rationnel d'ordre inifini de* (3.7). *Soit p un nombre premier tel que p divise d. Alors p divise $\widehat{\Psi}_m$ si et seulement si p divise m, c'est-à-dire si $r = r(p) = p$. De plus,* $\nu_p(\widehat{\Psi}_p) = 1$.

Preuve. — En utilisant les propriétés de $\Psi_m(M)$, on obtient :

$$\Psi_m(M) = \begin{cases} mx^{\frac{1}{2}(m^2-1)-1} + \alpha_{\frac{1}{2}(m^2-1)-1}x^{\frac{1}{2}(m^2-1)-1} \\ \qquad\qquad + \cdots + \alpha_0 \quad \text{si } m \text{ est impair}, \\ (2y + A_1x + A_3)\Big\{\frac{1}{2}mx^{\frac{1}{2}(m^2-4)} \\ \qquad\qquad +\beta_{\frac{1}{2}(m^2-4)-1}x^{\frac{1}{2}(m^2-4)-1} \\ \qquad\qquad\qquad + \cdots + \beta_0\Big\} \\ \qquad\qquad\qquad \text{si } m \text{ est pair}. \end{cases}$$

D'où :

$$
(3.8)\quad \Psi_m(M) = \begin{cases} ma^{\frac{1}{2}(m^2-1)} + \alpha_{\frac{1}{2}(m^2-1)-1} d^2 a^{\frac{1}{2}(m^2-1)-1} \\ \qquad\qquad + \cdots + \alpha_0 d^{m^2-1} \quad \text{si } m \text{ est impair,} \\ (2b + A_1 ad + A_3 d^3)\Big\{ \frac{1}{2} m a^{\frac{1}{2}(m^2-4)} \\ \qquad\qquad + \beta_{\frac{1}{2}(m^2-4)-1} d^2 a^{\frac{1}{2}(m^2-4)-1} \\ \qquad\qquad + \cdots + \beta_0 d^{m^2-4}\Big\} \\ \qquad\qquad \text{si } m \text{ est pair.} \end{cases}
$$

On conclut facilement la démonstration. □

Si maintenant p ne divise pas d, alors $M \pmod p) \neq \infty$ et $M \in E(\mathbb{F}_p)_{n.s.}$. Il est clair que $r = r(p) =$ ordre de M dans le groupe $E(\mathbb{F}_p)_{n.s}$.

- Si la courbe a bonne réduction en p, Hasse a montré que

$$
\left|E(\mathbb{F}_p)\right| < p + 1 + 2\sqrt{p}
$$

donc $r < p + 1 + 2\sqrt{p}$.

- Si la courbe a mauvaise réduction en p :

$$
\left|E(\mathbb{F}_p)_{n.s.}\right| = \begin{cases} p \quad \text{si } p \text{ est impair et si la courbe a une réduction additive sur } \mathbb{F}_p\,; \\ 2 \text{ ou } 4 \quad \text{si } p = 2 \text{ et si la courbe a une réduction additive sur } \mathbb{F}_p\,; \\ p-1 \text{ ou } p+1 \quad \text{dans le cas où la réduction sur } \mathbb{F}_p \text{ est multiplicative.} \end{cases}
$$

Dans tous les cas, on a donc $r = r(p) < p + 1 + 2\sqrt{p}$.

Nous allons maintenant démontrer le théorème B caractérisant l'ordre d'apparition de p^e dans la suite $(\widehat{\Psi}_m)$.

Preuve du théorème B.

Pour tout entier $m \neq 0$, on pose $m = r^{h_0} p^{h_1} n$ avec $h_1 \geq 0$ et $(p, n) = 1$. On a $h_0 = 0$ si r ne divise pas m et $h_0 = 1$ si r divise m. Nous allons montrer que

$$
\nu_p(\widehat{\Psi}_m) = \begin{cases} 0 & \text{si } h_0 = 0, \\ h_1 + \nu_p(\widehat{\Psi}_r) & \text{si } h_0 = 1. \end{cases}
$$

- Si $h_0 = 0$, le résultat est clair d'après la discussion précédente.
- Si $h_0 = 1$ et $m = rp^{h_1}n$, on procède par récurrence sur h_1.

a) Supposons que $h_1 = 0$ et $m = rn$. On a d'après (3.6) :

$$\begin{aligned}\Psi_{rn}^2(M) &= \Psi_r^{2n^2}(M)\Psi_n^2(rM)\\ &= \Psi_r^{2n^2}(M)\Big[n^2\Big(\frac{\phi_r(M)}{\Psi_r^2(M)}\Big)^{n^2-1} + \cdots + c_0\Big]\\ &= \Psi_r^2(M)\Big[n^2\phi_r^{n^2-1}(M) + \cdots + c_0(\Psi_r^2(M))^{n^2-1}\Big].\end{aligned}$$

Le crochet représente une forme binaire en $\Psi_r^2(M)$, $\phi_r(M)$, de degré n^2-1. En multipliant cette égalité par $d^{2(r^2n^2-1)}$, on obtient :

$$\widehat{\Psi}_{rn}^2 = \widehat{\Psi}_r^2\Big[n^2\widehat{\phi}_r^{n^2-1} + c_{n^2-2}d^4\widehat{\phi}_r^{n^2-2}\,\widehat{\Psi}_r^2 + \cdots + c_0 d^{2n^2-2}(\widehat{\Psi}_r^2)^{n^2-1}\Big].$$

Comme p divise $\widehat{\Psi}_r$, le théorème A montre que $(p,\widehat{\phi}_r) = 1$. De plus $(p,n) = 1$, d'où $\nu_p(\widehat{\Psi}_{rn}^2) = \nu_p(\widehat{\Psi}_r^2)$ et $\nu_p(\widehat{\Psi}_{rn}) = \nu_p(\widehat{\Psi}_r)$, ce qui fonde la récurrence.

b) Supposons que $h_1 \geq 0$ et que $\nu_p(\widehat{\Psi}_{rp^{h_1}n}) = h_1 + \nu_p(\widehat{\Psi}_r)$ et montrons que $\nu_p(\widehat{\Psi}_{rp^{h_1+1}n}) = e_1 + 1 + \nu_p(\widehat{\Psi}_r)$. Posons $k = rp^{h_1}n$. D'après (3.6), on a

$$\begin{aligned}\widehat{\Psi}_m^2(M) = \widehat{\Psi}_k^2(M)\Big[&p^2\widehat{\phi}_k^{p^2-1}(M) + s_{p-2}d^4\phi_k^{p^2-2}(M)\widehat{\Psi}_k^2(M)\\ &+ \cdots + s_0 d^{2p^2-2}(\widehat{\Psi}_k^2)^{p^2-1}\Big]\end{aligned}$$

où p divise s_{p-2}. Puisque p divise $\widehat{\Psi}_k(M)$, il est clair que la valuation des termes figurant dans le crochet à partir du deuxième est supérieure ou égale à 3. Comme p ne divise pas $\widehat{\phi}_k(M)$, on en déduit que la valuation du crochet vaut 2. D'où $\nu_p(\widehat{\Psi}_{pk}^2) = \nu_p(\widehat{\Psi}_k^2) + 2$ et par suite $\nu_p(\widehat{\Psi}_{pk}) = \nu_p(\widehat{\Psi}_k) + 1 = h_1 + 1 + \nu_p(\widehat{\Psi}_r)$. □

4. Périodicité des suites elliptiques.

Soit M un point rationnel d'ordre infini sur la courbe :

(4.1) $$y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6, \qquad A_i \in \mathbb{Z}.$$

Soit q un nombre entier ≥ 2, tel que $M \pmod p$ est non singulier pour tout nombre premier p divisant q. On a le :

LEMME 2. — *Soit* $q = p_1^{h_1} \cdots p_s^{h_s}$ *la factorisation de* q *en facteurs irréductibles. Alors la suite* $(\widehat{\Psi}_m)$ *est périodique* (mod q) *si et seulement si* $(\widehat{\Psi}_m)$ *est périodique* (mod $p_i^{e_i}$) *pour* $i = 1, \dots, s$. *Dans ce cas, on a* $\pi(q) = \mathrm{ppcm}(\pi(p_1^{e_1}), \dots \pi(p_s^{e_s}))$.

On peut donc se borner à étudier la périodicité (mod p^e) lorsque p est un nombre premier tel que M (mod p) est non singulier et e un entier ≥ 1. Supposons que p est impair et soient r l'ordre d'apparition de p et r_e celui de p^e dans la suite $(\widehat{\Psi}_m)$. On suppose que $r \geq 3$.

Preuve du théorème C.

Pour tout $(n, k) \in \mathbb{Z} \times \mathbb{Z}$, on doit démontrer que

$$\widehat{\Psi}_{kr_e+n} \equiv a_e^{kn} b_e^{k^2} \widehat{\Psi}_n \pmod{p^e} \tag{4.2}$$

avec $a_e = \widehat{\Psi}_{r_e+2}/\widehat{\Psi}_2\widehat{\Psi}_{r_e+1}$ et $b_e = \widehat{\Psi}_{r_e+1}^2\widehat{\Psi}_2/\widehat{\Psi}_{r_e+2}$.

1) *On commence par démontrer* (4.2) *pour* $k = 1$ *et* $n \geq 0$.

a) Pour $n = 0$, on a $\widehat{\Psi}_{r_e} \equiv 0$ (mod p^e) et $\widehat{\Psi}_0 = 0$, donc (4.2) est vraie pour $n = 0$. Ensuite, $\widehat{\Psi}_{r_e+1} = a_e b_e$ et $\widehat{\Psi}_{r_{e+2}} = a_e^2 b_e \widehat{\Psi}_2$, donc (4.2) est vérifiée pour $n = 1$ et $n = 2$.

On fait la démonstration pour $n = 3$ et 4 en posant $h = \nu_p(d)$, $h \geq 0$. De plus, en traduisant que mM est sur la courbe (4.1), il vient :

$$\begin{aligned}
&\widehat{\omega}_m^2(\widehat{\Psi}_m^3) + A_1 d\widehat{\omega}_m(\widehat{\phi}_m\widehat{\Psi}_m)(\widehat{\Psi}_m^3) + A_3 d^3\widehat{\omega}_m(\widehat{\Psi}_m^3)^2 \\
&\quad = (\widehat{\phi}_m\widehat{\Psi}_m)^3 + A_2 d^2(\widehat{\phi}_m\widehat{\Psi}_m)^2(\widehat{\Psi}_m^3) + A_4 d^4(\widehat{\phi}_m\widehat{\Psi}_m)(\widehat{\Psi}_m^3)^2 + A_6 d^6(\widehat{\Psi}_m^3)^3.
\end{aligned}$$

En désignant par $\widehat{M}$ le point $\widehat{M} = (a, b)$, cela montre que $w_m = \widehat{\Psi}_m^3$, $u_m = \widehat{\phi}_m\widehat{\Psi}_m$, $v_m = \widehat{\omega}_m$ sont les coordonnées homogènes de $m\widehat{M}$ sur la courbe

$$v^2 w + A_1 duvw + A_3 d^3 vw^2 = u^3 + A_2 d^2 u^2 w + A_4 d^4 uw2 + A_6 d^6 w^3.$$

Considérons cette courbe sur l'anneau $\mathbb{Z}/p^e\mathbb{Z}$. L'ensemble des points non singuliers de la courbe forme un groupe et l'ordre de $\widehat{M}$ dans ce groupe est le plus petit entier $m \geq 1$ tel que $w_m \equiv 0$ (mod p^e) et $u_m \equiv 0$ (mod p^e). Cet ordre est donc r_e. On en déduit que pour tout entier m, on a

$$\begin{aligned}
\widehat{\Psi}_{r_{e+m}}^3 &\equiv \lambda_m \widehat{\Psi}_m^3, \\
\widehat{\phi}_{r_{e+m}}\widehat{\Psi}_{r_{e+m}} &\equiv \lambda_m \widehat{\phi}_m\widehat{\Psi}_m, \\
\widehat{\omega}_{r_{e+m}} &\equiv \lambda_m \widehat{\omega}_m \pmod{p^e},
\end{aligned}$$

avec $\lambda_m \in \mathbb{Z}$ et $(\lambda_m, p) = 1$. En particulier pour $m = 2$, on a :

$$\begin{aligned}
&\widehat{\Psi}^3_{r_e+2} \equiv \lambda_2 \widehat{\Psi}^3_2,\\
&\widehat{\phi}_{r_e+2} \widehat{\Psi}_{r_e+2} \equiv \lambda_2 \widehat{\phi}_2 \widehat{\Psi}_2,\\
&\widehat{\omega}_{r_e+2} \equiv \lambda_2 \widehat{\omega}_2 \pmod{p^e}, \quad (\lambda_2, p) = 1.
\end{aligned}$$

On en déduit que :

$$\tag{4.3} \begin{cases} \widehat{\phi}_{r_e+2}/\widehat{\Psi}^2_{r_e+2} \equiv \widehat{\phi}_2 \widehat{\Psi}^2_2 \pmod{p^e}, \\ \widehat{\omega}_{r_e+2} \widehat{\Psi}^3_{r_e+2} \equiv \widehat{\omega}_2 \widehat{\Psi}^3_2 \pmod{p^e}. \end{cases}$$

D'après (3.4), la première relation donne :

$$\frac{a\widehat{\Psi}^2_{r_e+2} - \widehat{\Psi}_{r_e+1}\widehat{\Psi}_{r_e+3}}{\widehat{\Psi}^2_{r_e+2}} \equiv \frac{a\widehat{\Psi}^2_2 - \widehat{\Psi}_1\widehat{\Psi}_3}{\widehat{\Psi}^2_2} \pmod{p^e}.$$

Comme $\widehat{\Psi}_1 = 1$, on obtient $\widehat{\Psi}_{r_e+1}\widehat{\Psi}_{r_e+3}/\widehat{\Psi}^2_{r_e+2} \equiv \widehat{\Psi}_3/\widehat{\Psi}^2_2 \pmod{p^e}$, d'où

$$\begin{aligned}
\widehat{\Psi}_{r_e+3} &\equiv \widehat{\Psi}^2_{r_e+2}\widehat{\Psi}_3/\widehat{\Psi}_{r_e+1}\widehat{\Psi}^2_2 \pmod{p^e}\\
&\equiv (a_e^2 b_e \widehat{\Psi}_2)^2 / a_e b_e \widehat{\Psi}^2_2\\
&\equiv a_e^3 b_e \widehat{\Psi}_3 \pmod{p^e},
\end{aligned}$$

ce qui démontre (4.2) pour $n = 3$.

De plus, on a

$$\begin{aligned}
\omega_m &= \frac{\Psi_{2m}}{2\Psi_m} - \frac{1}{2}\Psi_m(A_1\phi_m + A_3\Psi^2_m)\\
&= \frac{\Psi_{m+2}\Psi^2_{m-1} - \Psi_{m-2}\Psi^2_{m+1}}{2\Psi_2} - \frac{1}{2}\Psi_m(A_1\phi_m + A_3\Psi^2_m),
\end{aligned}$$

d'où

$$\widehat{\omega}_m = \frac{\widehat{\Psi}_{m+2}\widehat{\Psi}^2_{m-1} - \widehat{\Psi}_{m-2}\widehat{\Psi}^2_{m+1}}{2\widehat{\Psi}_2} - \frac{1}{2}\widehat{\Psi}_m\Big[dA_1(a\widehat{\Psi}^2_m - \widehat{\Psi}_{m-1}\widehat{\Psi}_{m+1}) + A_3 d^3 \widehat{\Psi}^2_m\Big],$$

$$\begin{aligned}
\frac{\widehat{\omega}_m}{\widehat{\Psi}^3_m} &= \frac{\widehat{\Psi}_{m+2}\widehat{\Psi}^2_{m-1} - \widehat{\Psi}_{m-2}\widehat{\Psi}^2_{m+1}}{2\widehat{\Psi}_2\widehat{\Psi}^3_m} - \frac{1}{2}\Big[dA_1(a - \widehat{\Psi}_{m-1}\widehat{\Psi}_{m+1}/\widehat{\Psi}^2_m) + A_3 d^3\Big]\\
&= \frac{\widehat{\Psi}_{m+2}\widehat{\Psi}^2_{m-1} - \widehat{\Psi}_{m-2}\widehat{\Psi}^2_{m+1}}{2\widehat{\Psi}_2\widehat{\Psi}^3_m} - \frac{1}{2}(dA_1 a + A_3 d^3) + \frac{dA_1\widehat{\Psi}_{m-1}\widehat{\Psi}_{m+1}}{2\widehat{\Psi}^2_m}.
\end{aligned}$$

Or, pour $m = r_e + 2$, on obtient :

$$\frac{\widehat{\omega}_{r_{e+2}}}{\widehat{\Psi}^3_{r_{e+2}}} = \frac{\widehat{\Psi}_{r_{e+4}}\widehat{\Psi}^2_{r_{e+1}} - \widehat{\Psi}_{r_e}\widehat{\Psi}^2_{r_{e+3}}}{2\widehat{\Psi}_2\widehat{\Psi}^3_{r_{e+2}}} - \frac{1}{2}(A_1ad + A_3d^3) + \frac{dA_1\widehat{\Psi}_{r_{e+1}}\widehat{\Psi}_{r_{e+3}}}{2\widehat{\Psi}^2_{r_{e+2}}}.$$

De même, pour $m = 2$ on obtient :

$$\frac{\widehat{\omega}_2}{\widehat{\Psi}^3_2} = \frac{\widehat{\Psi}_4\widehat{\Psi}^2_1 - \widehat{\Psi}_0\widehat{\Psi}^2_3}{2\Psi^4_2} - \frac{1}{2}(A_1ad + A_3d^3) + \frac{1}{2}dA_1\widehat{\Psi}_1\widehat{\Psi}_3/\widehat{\Psi}^2_2.$$

En utilisant la deuxième relation contenue dans (4.3) et en tenant compte de $\widehat{\Psi}_0 = 0$, $\widehat{\Psi}_1 = 1$, $\widehat{\Psi}_{r_e} \equiv 0 \pmod{p^e}$, on obtient :

$$\frac{\widehat{\Psi}_{r_{e+4}}\widehat{\Psi}^2_{r_{e+1}}}{2\widehat{\Psi}_2\widehat{\Psi}^3_{r_{e+2}}} + \frac{1}{2}\frac{dA_1\widehat{\Psi}_{r_{e+1}}\widehat{\Psi}_{r_{e+3}}}{2\widehat{\Psi}^2_{r_{e+2}}} \equiv \widehat{\Psi}_4/2\widehat{\Psi}^4_2 + \frac{1}{2}\frac{dA_1\widehat{\Psi}_3}{2\widehat{\Psi}^2_2} \pmod{p^e}$$

d'où

$$\frac{\widehat{\Psi}_{r_{e+4}}(a_eb_e)^2}{2\widehat{\Psi}_2(a_e^2b_e\widehat{\Psi}_2)^3} + \frac{1}{2}\frac{dA_1a_eb_ea_e^3\widehat{\Psi}_3}{2(a_e^2b_e\widehat{\Psi}_2)^2} \equiv \frac{\Psi_4}{2\widehat{\Psi}^4_2} + \frac{1}{2}\frac{dA_1\widehat{\Psi}_3}{2\widehat{\Psi}^2_2} \pmod{p^e}$$

et par suite

$$\frac{\widehat{\Psi}_{r_{e+4}}}{2\widehat{\Psi}^4_2a_e^4b_e} + \frac{1}{2}\frac{dA_1\widehat{\Psi}_3}{2\widehat{\Psi}^2_2} \equiv \frac{\Psi_4}{2\widehat{\Psi}^4_2} + \frac{1}{2}\frac{dA_1\widehat{\Psi}_3}{2\widehat{\Psi}^2_2} \pmod{p^e},$$

d'où $\widehat{\Psi}_{r_{e+4}} \equiv a_e^4b_e\widehat{\Psi}_4 \pmod{p^e}$, ce qui démontre (4.2) pour $n = 4$.

b) Soit $n > 4$. On suppose que (4.2) est vraie pour tout i tel que $0 \leq i < n$. On va la démontrer pour n en utilisant la relation suivante déjà signalée dans le paragraphe 3 et numérotée (3.5) :

$$\widehat{\Psi}_{u+v}\widehat{\Psi}_{u-v} = \widehat{\Psi}_{u+1}\widehat{\Psi}_{u-1}\widehat{\Psi}^2_v - \widehat{\Psi}_{v+1}\widehat{\Psi}_{v-1}\widehat{\Psi}^2_u. \tag{4.4}$$

• Si $n = 2k+1$ est impair, on prend $u = r_e + k + 1$ et $v = k$. On obtient :

$$\widehat{\Psi}_{r_{e+2k+1}}\widehat{\Psi}_{r_{e+1}} = \widehat{\Psi}_{r_{e+k+2}}\widehat{\Psi}_{r_{e+k}}\widehat{\Psi}^2_k - \widehat{\Psi}_{k+1}\widehat{\Psi}_{k-1}\widehat{\Psi}^2_{r_{e+k+1}}.$$

Comme $n > 4$, on a $k < k+1 < k+2 < 2k+1 = n$, de sorte que l'hypothèse de récurrence s'applique aux entiers k, $k+1$ et $k+2$, d'où

$$\begin{aligned}&\widehat{\Psi}_{r_{e+2k+1}} a_e b_e \widehat{\Psi}_1 \\ &\qquad \equiv a_e^{k+2} b_e \widehat{\Psi}_{k+2} a_e^k b_e \Psi_k^3 - \widehat{\Psi}_{k+1} \widehat{\Psi}_{k-1} a_e^{2(k+1)} b_e^2 \widehat{\Psi}_{k+1}^3 \pmod{p^e}\end{aligned}$$

et donc :

$$\widehat{\Psi}_{r_{e+2k+1}} \equiv a_e^{2k+1} b_e (\widehat{\Psi}_{k+2} \Psi_k^3 - \widehat{\Psi}_{k-1} \widehat{\Psi}_{k+1}^3) \equiv a_e^{2k+1} b_e \widehat{\Psi}_{2k+1} \pmod{p^e}.$$

• Si $n = 2k$ est pair, on prend $u = r_e + k + 1$ et $v = k - 1$ dans (4.4). On obtient :

$$\widehat{\Psi}_{r_{e+2k}} \widehat{\Psi}_{r_{e+2}} = \widehat{\Psi}_{r_{e+k+2}} \widehat{\Psi}_{r_{e+k}} \widehat{\Psi}_{k-1}^2 - \widehat{\Psi}_{k-2} \widehat{\Psi}_k \widehat{\Psi}_{r_{e+k+1}}^2.$$

Comme précédemment, l'hypothèse de récurrence s'applique aux entiers k, $k+1$ et $k+2$. Donc

$$\begin{aligned}\widehat{\Psi}_{r_{e+2k}} a_e^2 b_e \widehat{\Psi}_2 &\equiv a_e^{k+2} b_e \widehat{\Psi}_{k+2} a_e^k b_e \widehat{\Psi}_k \widehat{\Psi}_{k-1}^2 \\ &\qquad - \widehat{\Psi}_{k-2} \widehat{\Psi}_k a_e^{2(k+1)} b_e^2 \widehat{\Psi}_{k+1}^2 \pmod{p^e},\end{aligned}$$

d'où

$$\widehat{\Psi}_{r_{e+2k}} \equiv a_e^{2k} b_e \widehat{\Psi}_k \frac{\widehat{\Psi}_{k+2} \widehat{\Psi}_{k-1}^2 - \widehat{\Psi}_{k-2} \widehat{\Psi}_{k+1}^2}{\Psi_2} \equiv a_e^{2k} b_e \widehat{\Psi}_{2k} \pmod{p^e},$$

ce qui achève la démonstration du théorème dans le cas où $k = 1$ et $n \geq 0$.

Avant de poursuivre la démonstration du théorème C dans le cas où $k = 1$ et $n < 0$ prouvons d'abord le :

LEMME 3. — *On a* $a_e^{r_e} b_e^{-2} \equiv 1 \pmod{p^e}$ *et* $\widehat{\Psi}_{r_{e-1}} \equiv -a_e^{-1} b_e \pmod{p^e}$.

Preuve. — On a :

$$\widehat{\Psi}_{2r_{e+1}} = \widehat{\Psi}_{r_{e+2}} \widehat{\Psi}_{r_e}^3 - \widehat{\Psi}_{r_{e-1}} \widehat{\Psi}_{r_{e+1}}^3 \equiv -\widehat{\Psi}_{r_{e-1}} \widehat{\Psi}_{r_{e+1}}^3 \equiv -\widehat{\Psi}_{r_{e-1}} a_e^3 b_e^3 \pmod{p^e}.$$

D'autre part on a :

$$\widehat{\Psi}_{2r_{e+1}} = \widehat{\Psi}_{r_e+(r_e+1)} \equiv a_e^{r_e+1} b_e \widehat{\Psi}_{r_{e+1}} \equiv a_e^{r_e+1} b_e a_e b_e \widehat{\Psi}_1 \equiv a_e^{r_e+2} b_e^2 \pmod{p^e}.$$

On en déduit que $\widehat{\Psi}_{r_{e-1}} \equiv -a_e^{r_e-1} b_e^{-1} \pmod{p^e}$. De plus, on a

$$\begin{aligned}\widehat{\Psi}_{r_e+r_{e-1}} &= \widehat{\Psi}_{2r_{e-1}} = \widehat{\Psi}_{2(r_{e-1})+1} \\ &= \Psi_{r_{e+1}} \Psi_{r_{e-1}}^3 - \widehat{\Psi}_{r_{e-1}} \widehat{\Psi}_{r_e}^3 \\ &\equiv \widehat{\Psi}_{r_{e+1}} \widehat{\Psi}_{r_{e-1}}^3 \pmod{p^e},\end{aligned}$$

donc $a_e^{r_{e-1}} b_e \widehat{\Psi}_{r_{e-1}} \equiv \widehat{\Psi}_{r_{e+1}} \widehat{\Psi}^3_{r_{e-1}} \pmod{p^e}$, d'où

$$a_e^{r_{e-1}} b_e \equiv a_e b_e (-a_e^{r_{e-1}} b_e^{-1})^2 \pmod{p^e}$$

et par suite $a_e^{r_e} b_e^{-2} \equiv 1 \pmod{p^e}$. On en déduit que $\widehat{\Psi}_{r_{e-1}} \equiv -a_e^{-1} b_e \pmod{p^e}$.

2) *Suite de la démonstration du théorème C dans le cas où $k = 1$ et $n < 0$.*

La relation (4.2) est vraie pour $n = -1$ d'après le lemme précédent. Montrons qu'elle est vraie pour $n < -1$. Si r_e divise n, alors (4.2) est vraie d'après le théorème B. Supposons donc que r_e ne divise pas n.

• Si r ne divise pas n, alors r ne divise pas $r_e \pm n$. D'après le théorème B, on a $\nu_p(\widehat{\Psi}_{r_{e+n}}) = \nu_p(\widehat{\Psi}_{r_{e-n}}) = \nu_p((\widehat{\Psi}_n) = 0$.

• Si r divise n, on pose $n = rp^h n'$ avec $h \geq 0$, $(p, n') = 1$ et $r_e = rp^k$ avec $k > h$ car r_e ne divise pas n. On en déduit que $r_e \pm n = rp^k \pm rp^h n' = rp^h(p^{k-h} \pm n')$, ce qui montre que $(p, p^{k-h} \pm n') = 1$. Le théorème B (ii) montre alors que :

$$\nu_p(\widehat{\Psi}_{r_{e+n}}) = \nu_p(\widehat{\Psi}_{r_{e-n}}) = \nu_p(\widehat{\Psi}_n).$$

Si r_e ne divise pas n, on en conclut $\nu_p(\widehat{\Psi}_{r_{e+n}}) = \nu_p(\widehat{\Psi}_{r_{e-n}}) = \nu_p(\widehat{\Psi}_n) < e$. Par application de (4.2) pour $-n$, on a maintenant :

$$\widehat{\Psi}_{r_{e-n}} \equiv a_e^{-n} b_e \widehat{\Psi}_{-n} \pmod{p^e} \equiv -a_e^{-n} b_e \widehat{\Psi}_n \pmod{p^e}.$$

Multiplions cette congruence par $\widehat{\Psi}_{r_{e+n}}$. On obtient :

$$\begin{aligned}\widehat{\Psi}_{r_{e-n}} \widehat{\Psi}_{r_{e+n}} &\equiv a_e^{-n} b_e \widehat{\Psi}_n \widehat{\Psi}_{r_{e+n}} \pmod{p^{e+\nu_p(\widehat{\Psi}_{r_{e+n}})}} \\ &\equiv -a_e^{-n} b_e \widehat{\Psi}_n \widehat{\Psi}_{r_{e+n}} \pmod{p^{e+\nu_p(\widehat{\Psi}_n)}}.\end{aligned}$$

Comme $\nu_p(\widehat{\Psi}_n) < e$, d'après (4.4), on a :

$$\begin{aligned}\widehat{\Psi}_{r_{e+n}} \widehat{\Psi}_{r_{e-n}} &= \widehat{\Psi}_{r_{e-1}} \widehat{\Psi}_{r_{e+1}} \widehat{\Psi}_n^2 - \widehat{\Psi}_{n-1} \widehat{\Psi}_{n+1} \widehat{\Psi}_r^2 \\ &\equiv \widehat{\Psi}_{r_{e-1}} \widehat{\Psi}_{r_{e+1}} \widehat{\Psi}_n^2 \pmod{p^{2e}} \\ &\equiv \widehat{\Psi}_{r_{e-1}} \widehat{\Psi}_{r_{e+1}} \widehat{\Psi}_n^2 \pmod{p^{e+\nu_p(\widehat{\Psi}_n)}}.\end{aligned}$$

En comparant les deux congruences vérifiées par $\widehat{\Psi}_{r_{e-n}}\widehat{\Psi}_{r_{e+n}}$, on en conclut que $-a_e^{-n}b_e\widehat{\Psi}_n\widehat{\Psi}_{r_{e+n}} \equiv \widehat{\Psi}_{r_{e-1}}\widehat{\Psi}_{r_{e+1}}\widehat{\Psi}_n^2 \pmod{p^{e+\nu_p(\widehat{\Psi}_n)}}$. Après division par $\widehat{\Psi}_n$, on obtient $-a_e^{-n}b_e\widehat{\Psi}_{r_{e+n}} \equiv \widehat{\Psi}_{r_{e-1}}\widehat{\Psi}_{r_{e+1}}\widehat{\Psi}_n \pmod{p^e}$. En appliquant le lemme précédent et (4.2) pour $n = 1$, on a :

$$\widehat{\Psi}_{r_{e+n}} \equiv a_e^n b_e \widehat{\Psi}_n \pmod{p^e},$$

ce qui achève la preuve du théorème C dans le cas où $k = 1$.

3) *Preuve de* (4.2) *dans le cas général.*

Supposons que (4.2) est démontrée pour $k \geq 0$ et soit $k < 0$. On a

$$\widehat{\Psi}_{kr_{e+n}} = -\widehat{\Psi}_{(-k)r_{e-n}} \equiv -a_e^{(-k)(-n)}b_e^{k^2}\widehat{\Psi}_{-n} \equiv a_e^{kn}b_e^{k^2}\widehat{\Psi}_n \pmod{p^e}$$

ce qui montre que (4.2) est démontrée pour k. On complète la démonstration pour $k \geq 0$ par récurrence sur k, en utilisant le lemme 3. □

Remarque 1. — Plaçons-nous dans le cas où p divise d et soit $h = \nu_p(d)$. Supposons que $e \leq 2h$. Alors :

$$a_e \equiv a^{p^e} \pmod{p^e}, \quad b_e \equiv \big(b + \tfrac{1}{2}A_1 ad\big)a^{\frac{1}{2}(p^{2e}-3)} \pmod{p^e}.$$

Preuve. — Reprenons la formule (3.8) utilisée dans le paragraphe 3 :

$$\widehat{\Psi}_m = \begin{cases} ma^{\frac{1}{2}(m^2-1)} + \alpha_{\frac{1}{2}(m^2-1)-1}d^2a^{\frac{1}{2}(m^2-1)-1} + \cdots + \alpha_0 d^{m^2-1} \\ \hfill \text{si m est pair,} \\ (2b + A_1ad + A_3d^3)\Big(\frac{1}{2}ma^{\frac{1}{2}(m^2-4)} + \beta_{\frac{1}{2}(m^2-4)-1}d^2a^{\frac{1}{2}(m^2-4)-1} \\ \hfill + \cdots + \beta_0 d^{m^2-4}\Big) \\ \hfill \text{si m est pair.} \end{cases}$$

Cela montre que :

$$\widehat{\Psi}_m \equiv \begin{cases} ma^{\frac{1}{2}(m^2-1)} \pmod{p^{2h}} & \text{si } m \text{ est impair,} \\ \frac{1}{2}m(2b + A_1ad)a^{\frac{1}{2}(m^2-4)} \pmod{p^{2h}} & \text{si } m \text{ est pair.} \end{cases}$$

Puisque l'ordre d'apparition de p^e dans $(\widehat{\Psi}_m)$ est $r_e = p^e$ (cf. § 3), on a :

$$\begin{aligned} \widehat{\Psi}_{r_{e+1}} &= \widehat{\Psi}_{p^e+1} \\ &\equiv a_eb_e \equiv (p^e+1)(b + \tfrac{1}{2}A_1ad)a^{\frac{1}{2}((p^e+1)^2-4)} \\ &\equiv (b + \tfrac{1}{2}A_1ad)a^{\frac{1}{2}((p^e+1)^2-4)} \pmod{p^e}, \end{aligned}$$

$$\begin{aligned}\widehat{\Psi}_{r_{e+2}} &= \widehat{\Psi}_{p^e+2} \\ &\equiv a_e^2 b_e \widehat{\Psi}_2 \equiv (p^e+2) a^{\frac{1}{2}((p^e+2)^2-1)} \\ &\equiv 2\, a^{\frac{1}{2}((p^e+2)^2-1)} \pmod{p^e}.\end{aligned}$$

On en déduit que $a_e \equiv 2\, a^{p^e+3}/(b+\frac{1}{2}A_1ad)\widehat{\Psi}_2 \pmod{p^e}$. Or

$$\widehat{\Psi}_2 = 2b + A_1ad + A_3d^3 \equiv 2(b+\tfrac{1}{2}A_1ad) \pmod{p^e}.$$

Donc $a_e \equiv a^{p^e+3}/(b^2+A_1abd) \pmod{p^e}$. Or

$$b^2 + A_1abd + A_3bd^3 = a^3 + A_2a^2d^2 + A_4ad^4 + A_6d^6.$$

Donc $b^2 + A_1abd \equiv a^3 \pmod{p^e}$, d'où $a_e \equiv a^{p^e} \pmod{p^e}$ et par suite $b_e \equiv (b+\frac{1}{2}A_1ad)a^{p^{2e-3}/2} \pmod{p^e}$. □

Avant d'entreprendre la démonstration du théorème D, rappelons les notations déjà évoquées dans le paragraphe 2.

- Pour tout entier $e \geq 1$, on note $(\mathbb{Z}/p^e\mathbb{Z})^*$ le groupe des unités de $\mathbb{Z}/p^e\mathbb{Z}$.
- Pour tout $u \in \mathbb{Z}; (u,p) = 1$, on note $\theta_e(u)$ l'ordre de u dans le groupe $(\mathbb{Z}/p^e\mathbb{Z})^*$.

Preuve du théorème D.

Soit k_e le plus petit entier > 0 tel que

$$a_e^{k_e} \equiv 1 \pmod{p^e} \quad \text{et} \quad b_e^{k_e^2} \equiv 1 \pmod{p^e}. \tag{4.6}$$

D'après le théorème C, on a alors pour tout $n \in \mathbb{Z}$:

$$\widehat{\Psi}_{k_er_e+n} \equiv a_e^{k_en} b_e^{k_e2} \widehat{\Psi}_n \equiv \widehat{\Psi}_n \pmod{p^e}.$$

On en déduit que la suite $(\widehat{\Psi}_m)$ est périodique $\pmod{p^e}$ et k_er_e est une période de $\widehat{\Psi}_m \pmod{p^e}$. Désignons par π_e la période de $\widehat{\Psi}_m \pmod{p^e}$ (c'est-à-dire la plus petite période). On a évidemment $\pi_e \leq k_er_e$. De plus, π_e étant une période, on a $\widehat{\Psi}_{\pi_e+r_e} \equiv \widehat{\Psi}_{r_e} \equiv 0 \pmod{p^e}$ donc $r_e \mid \pi_e$. Posons $\pi_e = c_er_e$, avec $c_e \leq k_e$. On a :

$$\widehat{\Psi}_{\pi_e+n} \equiv \widehat{\Psi}_{c_er_e+n} \equiv a_e^{c_en} b_e^{c_e^2} \widehat{\Psi}_n \equiv \widehat{\Psi}_n \pmod{p^e}.$$

En faisant $n=1$ puis $n=2$, on obtient $a_e^{c_e} b_e^{c_e^2} \equiv 1$ et $a_e^{2c_e} b_e^{c_e^2} \equiv 1 \pmod{p^e}$, d'où $a_e^{c_e} \equiv 1$ et $b_e^{c_e^2} \equiv 1 \pmod{p^e}$ et par suite c_e vérifie (4.6). Comme k_e est minimal on a $k_e \leq c_e$ et finalement $k_e = c_e$ et $\pi_e = k_e r_e$.

Prouvons maintenant l'assertion sur le lien entre k_e et $\theta_e(a_e)$. La relation $a_e^{r_e} b_e^{-2} \equiv 1 \pmod{p^e}$ (prouvée dans le lemme 3) montre que $\theta_e(b_e)$ divise $2\theta_e(a_e)$, d'où $k_e \leq 2\theta_e(a_e)$. On a $a_e^{k_e} \equiv 1 \pmod{p^e}$ et $b_e^{k_e^2} \equiv 1 \pmod{p^e}$, donc $\theta_e(a_e)$ divise k_e. Finalement, on a $k_e = \theta_e(a_e)$ ou $k_e = 2\theta_e(a_e)$.

La dernière assertion du théorème D se démontre comme suit. Supposons que $k_e = 2\theta_e(a_e)$. Alors $\theta_e(b_e)$ ne divise pas $\theta_e(a_e)$. En tenant compte de $\theta_e(b_e) \mid 2\theta_e(a_e)$, posons $\theta_e(a_e) = 2^h u$, avec u impair et $\theta_e(b_e) = 2^{h+1}\, u'$ où u' divise u. Si $h \geq 1$, alors $b_e^{\theta_e^2(a_e)} = b_e^{2^{2h} u^2} \equiv 1 \pmod{p^e}$ car $h+1 \leq 2h$ et u' divise u, d'où $k_e = \theta_e(a_e)$, ce qui contredit l'hypothèse. On en déduit que $h=0$, $\theta_e(a_e)$ est impair, $\theta_e(b_e) = 2u'$ et u' divise u.

Réciproquement si $\theta_e(a_e)$ est impair et $\theta_e(b_e)$ pair alors $\theta_e(b_e)$ ne divise pas $\theta_e(a_e)$; donc $k_e = 2\theta_e(a_e)$ ce qui achève la preuve du théorème D.

Remarque 2. — Ward a énoncé le résultat suivant [12, th. 28.1]. Soit (h_n) une suite elliptique telle que h_2 et $h_3 \neq 0$. Alors chacune des conditions suivantes est nécessaire et suffisante pour que h_n soit périodique de période η.

(i) $h_{n+\eta} = h_n, \quad (n = 0, 1, \dots, \eta)$;

(ii) $h_{\eta-n} = -h_n, \quad (n = 0, \dots, \eta)$;

(iii) $h_{\eta/2+n} = -h_n, \quad (\eta \text{ pair}, n = 0, 1, \dots, \eta/2)$.

Le résultat reste vrai (d'après Ward) si on entend par périodicité la périodicité (mod m) et où les égalités (i), (ii), (iii) sont remplacées par des congruences (mod m) et où on suppose h_2 et h_3 premiers à m.

L'exemple qui suit montre que l'on doit faire des réserves sur la condition (iii). Considérons la suite elliptique construite à partir de la courbe $y^2 = x^3 + 5$ et du point $M = (-1, 2)$. La suite $(\widehat{\Psi}_m)$ est périodique (mod 5) de période $\eta = 10$ et on a, modulo 5 :

$$\widehat{\Psi}_0 = 0, \quad \widehat{\Psi}_1 = 1, \quad \widehat{\Psi}_2 = 4, \quad \widehat{\Psi}_3 \equiv 3, \quad \widehat{\Psi}_4 \equiv 3,$$

$$\widehat{\Psi}_5 \equiv 0, \quad \widehat{\Psi}_6 \equiv 2, \quad \widehat{\Psi}_7 \equiv 2, \quad \widehat{\Psi}_8 \equiv 1; \quad \widehat{\Psi}_9 \equiv 4.$$

On a $\widehat{\Psi}_{\eta/2+1} = \widehat{\Psi}_6 \equiv 2 \pmod 5$ et $\widehat{\Psi}_1 \equiv 1 \pmod 5$, ce qui contredit (iii).

En utilisant la méthode de démonstration utilisée pour le théorème C, on peut prouver le :

THÉORÈME 1. — *Soit π le plus petit entier $>$ 0 tel que :*

$$\widehat{\Psi}_\pi \equiv 0, \quad \widehat{\Psi}_{\pi+1} \equiv \widehat{\Psi}_1 = 1, \quad \widehat{\Psi}_{\pi+2} \equiv \widehat{\Psi}_2 \pmod{p^e}.$$

Alors π est la période de $(\widehat{\Psi}_m) \pmod{p^e}$.

5. Relation entre π_e et π_{e+1}.

On suppose que p est impair dans ce paragraphe. Les lemmes qui suivent serviront à démontrer le théorème E, mais ils peuvent aussi avoir un intérêt en eux-mêmes. Le lemme 5 sera d'ailleurs utilisé dans le paragraphe 6.

LEMME 4. — *Soit p un nombre premier impair. Pour tout $u \in \mathbb{Q}$, on note $\nu_p(u)$ la valuation en p de u. Soit $a \in \mathbb{Q}$. Alors on a :*

$$\nu_p(a-1) = e \geq 1 \implies \nu_p(a^{p^\ell} - 1) = e + \ell.$$

LEMME 5. — *Soient $k, \lambda, e \in \mathbb{Z}$, avec $e \geq 1$ tels que $r_e \nmid n$. On a :*

$$\widehat{\Psi}_{k\lambda r_{e+1}} \equiv (-\widehat{\Psi}_{\lambda r_{e-1}})^{\frac{1}{2}k(k-1)} (\widehat{\Psi}_{\lambda r_{e+1}})^{\frac{1}{2}k(k+1)} \pmod{p^{3e}},$$

$$\widehat{\Psi}_{k\lambda r_{e-1}} \equiv -(-\widehat{\Psi}_{\lambda r_{e-1}})^{\frac{1}{2}k(k+1)} (\widehat{\Psi}_{\lambda r_{e+1}})^{\frac{1}{2}k(k-1)} \pmod{p^{3e}},$$

$$\frac{\widehat{\Psi}_{k\lambda r_{e+n}}}{\widehat{\Psi}_n} \equiv (-\widehat{\Psi}_{\lambda r_{e-1}} \widehat{\Psi}_{\lambda r_{e+1}})^{\frac{1}{2}k(k-1)} \Big(\frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n}\Big)^k \ \Big(\mathrm{mod}\ p^{2(e-\nu_p(\widehat{\Psi}_n))}\Big),$$

$$\frac{\widehat{\Psi}_{k\lambda r_{e+n}}}{\widehat{\Psi}_n} \equiv \Big(-\frac{\widehat{\Psi}_{\lambda r_{e-n}}}{\widehat{\Psi}_n} \frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n}\Big)^{\frac{1}{2}k(k-1)} \Big(\frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n}\Big)^k \ \Big(\mathrm{mod}\ p^{3(e-\nu_p(\widehat{\Psi}_n))}\Big).$$

En particulier, si r ne divise pas n, on a :

$$\frac{\widehat{\Psi}_{k\lambda r_{e+n}}}{\widehat{\Psi}_n} \equiv \Big(-\widehat{\Psi}_{\lambda r_{e-1}} \widehat{\Psi}_{\lambda r_{e+1}}\Big)^{\frac{1}{2}k(k-1)} \Big(\frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n}\Big)^k \pmod{p^{2e}},$$

$$\frac{\widehat{\Psi}_{k\lambda r_{e+n}}}{\widehat{\Psi}_n} \equiv \Big(-\frac{\widehat{\Psi}_{\lambda r_{e-n}}}{\widehat{\Psi}_n} \frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n}\Big)^{\frac{1}{2}k(k-1)} \Big(\frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n}\Big)^k \pmod{p^{3e}}.$$

Preuve. — Les dernières relations, valables pour r divisant n, se déduisent immédiatement des précédentes puisque dans ce cas $\nu_p(\widehat{\Psi}_n) = 0$.

Supposons que r_e ne divise pas n et que le lemme est démontré pour $k \geq 0$ et soit k un entier < 0. En utilisant la relation $\widehat{\Psi}_m = -\widehat{\Psi}_{-m}$, on voit que les deux premières et la quatrième relations sont vraies pour k. Pour la troisième relation on procède comme suit. On prend $(u, v) = (n, \lambda r_e)$ dans la relation de récurrence (4.4). On obtient

$$\widehat{\Psi}_{n+\lambda r_e}\widehat{\Psi}_{n-\lambda r_e} = \widehat{\Psi}_{n+1}\widehat{\Psi}_{n-1}\widehat{\Psi}^2_{\lambda r_e} - \widehat{\Psi}_{\lambda r_e+1}\widehat{\Psi}_{\lambda r_e-1}\widehat{\Psi}^2_n,$$

d'où

$$\widehat{\Psi}_{n+\lambda r_e}\widehat{\Psi}_{n-\lambda r_e} \equiv -\widehat{\Psi}_{\lambda r_e+1}\widehat{\Psi}_{\lambda r_e-1}\widehat{\Psi}^2_n \pmod{p^{2e}}$$

et par suite

$$\frac{\widehat{\Psi}_{n+\lambda r_e}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{n-\lambda r_e}}{\widehat{\Psi}_n} \equiv -\widehat{\Psi}_{\lambda r_{e+1}}\widehat{\Psi}_{\lambda r_{e-1}} \pmod{p^{2(e-\nu_p(\widehat{\Psi}_n))}}$$

qui équivaut au cas particulier $k = -1$ de cette troisième relation. Cela étant prouvé, pour $k < 0$ on a

$$\begin{aligned}\frac{\widehat{\Psi}_{k\lambda r_{e+n}}}{\widehat{\Psi}_n} &= \frac{\widehat{\Psi}_{(-k)\lambda r_e-n}}{\widehat{\Psi}_{-n}}\\ &\equiv \left(-\widehat{\Psi}_{\lambda r_{e-1}}\widehat{\Psi}_{\lambda r_{e+1}}\right)^{-\frac{1}{2}k(-k-1)}\left(\frac{\widehat{\Psi}_{\lambda r_{e-n}}}{\widehat{\Psi}_{-n}}\right)^{-k} \pmod{p^{2(e-\nu_p(\widehat{\Psi}_n))}}\end{aligned}$$

puisqu'on a supposé que le lemme 5 est vrai pour $-k$ (car $-k > 0$). On en déduit que :

$$\frac{\widehat{\Psi}_{k\lambda r_{e+n}}}{\widehat{\Psi}_n} \equiv \left(-\widehat{\Psi}_{\lambda r_{e-1}}\widehat{\Psi}_{\lambda r_{e+1}}\right)^{\frac{1}{2}k(k+1)}\left(\frac{\widehat{\Psi}_{-\lambda r_{e+n}}}{\widehat{\Psi}_n}\right)^{-k} \pmod{p^{2(e-\nu_p(\widehat{\Psi}_n))}}.$$

Faisant appel au cas particulier $k = -1$ prouvé ci-dessus pour remplacer $\widehat{\Psi}_{n-\lambda r_e}/\widehat{\Psi}_n$ par $\widehat{\Psi}_{n+\lambda r_e}/\widehat{\Psi}_n$, on obtient

$$\begin{aligned}\frac{\widehat{\Psi}_{k\lambda r_{e+n}}}{\widehat{\Psi}_n} &\equiv \left(-\widehat{\Psi}_{\lambda r_{e-1}}\widehat{\Psi}_{\lambda r_{e+1}}\right)^{\frac{1}{2}k(k+1)}\left[-\Psi_{\lambda r_{e+1}}\Psi_{\lambda r_{e-1}}\left(\frac{\widehat{\Psi}_{n+\lambda r_e}}{\widehat{\Psi}_n}\right)^{-1}\right]^{-k}\\ &\equiv \left(-\widehat{\Psi}_{\lambda r_{e-1}}\widehat{\Psi}_{\lambda r_{e+1}}\right)^{\frac{1}{2}k(k+1)}\left(-\Psi_{\lambda r_{e+1}}\Psi_{\lambda r_{e-1}}\right)^{-k}\left(\frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n}\right)^{k}\\ &\equiv \left(-\widehat{\Psi}_{\lambda r_{e-1}}\widehat{\Psi}_{\lambda r_{e+1}}\right)^{\frac{1}{2}k(k-1)}\left(\frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n}\right)^{k} \pmod{p^{2(e-\nu_p(\widehat{\Psi}_n))}},\end{aligned}$$

ce qui démontre le lemme pour $k < 0$.

Démontrons maintenant le lemme pour $k \geq 0$. Les relations contenues dans le lemme 5 sont évidentes pour $k = 0$ ou 1. On peut donc supposer que $k \geq 2$. Pour les trois premières relations on procède comme suit.

Dans la relation de récurrence (4.4), nous prenons successivement (u, v) égal à

$$\big((k-1)\lambda r_{e+1}, \lambda r_e\big), \quad \big((k-1)\lambda r_{e-1}, \lambda r_e\big), \quad \big((k-1)\lambda r_{e+n}, \lambda r_e\big)$$

et nous obtenons :

$$\begin{aligned}
\widehat{\Psi}_{k\lambda r_{e+1}} \widehat{\Psi}_{(k-2)\lambda r_{e+1}} &= \widehat{\Psi}_{(k-1)\lambda r_{e+2}} \widehat{\Psi}_{(k-1)\lambda r_e} \widehat{\Psi}^2_{\lambda r_e} \\
&\qquad - \widehat{\Psi}_{\lambda r_{e-1}} \widehat{\Psi}_{\lambda r_{e+1}} \widehat{\Psi}^2_{(k-1)\lambda r_{e+1}}, \\
\widehat{\Psi}_{k\lambda r_{e-1}} \widehat{\Psi}_{(k-2)\lambda r_{e-1}} &= \widehat{\Psi}_{(k-1)\lambda r_e} \widehat{\Psi}_{(k-1)\lambda r_{e-2}} \widehat{\Psi}^2_{\lambda r_e} \\
&\qquad - \widehat{\Psi}_{\lambda r_{e-1}} \widehat{\Psi}_{\lambda r_{e+1}} \widehat{\Psi}^2_{(k-1)\lambda r_{e-1}} \\
\widehat{\Psi}_{k\lambda r_{e+n}} \widehat{\Psi}_{(k-2)\lambda r_{e+n}} &= \widehat{\Psi}_{(k-1)\lambda r_{e+n+1}} \widehat{\Psi}_{(k-1)\lambda r_{e+n-1}} \widehat{\Psi}^2_{\lambda r_e}, \\
&\qquad - \widehat{\Psi}_{\lambda r_{e-1}} \widehat{\Psi}_{\lambda r_{e+1}} \widehat{\Psi}^2_{(k-1)\lambda r_{e+n}}.
\end{aligned}$$

On en déduit que :

$$\begin{aligned}
\widehat{\Psi}_{k\lambda r_{e+1}} &\equiv -\widehat{\Psi}_{\lambda r_{e-1}} \widehat{\Psi}_{\lambda r_{e+1}} \widehat{\Psi}_{(k-1)\lambda r_{e+1}} / \widehat{\Psi}_{(k-2)\lambda r_{e+1}} \pmod{p^{3e}}, \\
\widehat{\Psi}_{k\lambda r_{e-1}} &\equiv -\widehat{\Psi}_{\lambda r_{e-1}} \widehat{\Psi}_{\lambda r_{e+1}} \widehat{\Psi}_{(k-1)\lambda r_{e-1}} / \widehat{\Psi}_{(k-2)\lambda r_{e-1}} \pmod{p^{3e}}, \\
\frac{\widehat{\Psi}_{k\lambda r_{e+n}}}{\widehat{\Psi}_n} &\equiv \frac{\Big(\widehat{\Psi}_{\lambda r_{e-1}} \widehat{\Psi}_{\lambda r_{e+1}}\Big)\Big(\widehat{\Psi}_{(k-1)\lambda r_{e+n}} / \Psi_n\Big)^2}{\widehat{\Psi}_{(k-2)\lambda r_{e+n}} / \widehat{\Psi}_n} \ \Big(\mathrm{mod}\ p^{2(e - \nu_p(\widehat{\Psi}_n))}\Big).
\end{aligned}$$

On continue la démonstration par récurrence sur k. Pour la quatrième relation, on utilisera la formule de récurrence à trois indices suivante :

$$\widehat{\Psi}_{u+v} \widehat{\Psi}_{u-v} \widehat{\Psi}^2_t = \widehat{\Psi}_{u+t} \widehat{\Psi}_{u-t} \widehat{\Psi}^2_v - \widehat{\Psi}_{v+t} \widehat{\Psi}_{v-t} \widehat{\Psi}^2_u.$$

(Cette formule se déduit de (4.4) en remplaçant $\widehat{\Psi}_{u+t}\widehat{\Psi}_{u-t}$ et $\widehat{\Psi}_{v+t}\widehat{\Psi}_{v-t}$ par leurs valeurs, et reste valable en remplaçant Ψ_m par $\widehat{\Psi}_m$ pour $m = u, v, t$, $u \pm v$ $u \pm t$, $v \pm t$.) Prenons dans cette formule $v = \lambda r_e$, $u = (k-1)\lambda r_e + n$ et $t = n$. Nous obtenons

$$\begin{aligned}
\widehat{\Psi}_{k\lambda r_{e+n}} \widehat{\Psi}_{(k-2)\lambda r_{e+n}} \widehat{\Psi}^2_n &= \widehat{\Psi}_{(k-1)\lambda r_{e+2n}} \widehat{\Psi}_{(k-1)\lambda r_e} \widehat{\Psi}^2_{\lambda r_e} \\
&\qquad - \widehat{\Psi}_{\lambda r_{e+n}} \widehat{\Psi}_{\lambda r_{e-n}} \widehat{\Psi}^2_{(k-1)\lambda r_{e+n}},
\end{aligned}$$

d'où

$$\frac{\widehat{\Psi}_{k\lambda r_{e+n}}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{(k-2)\lambda r_{e+n}}}{\widehat{\Psi}_n} = \frac{\widehat{\Psi}_{(k-1)\lambda r_{e+2n}}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{(k-1)\lambda r_e}}{\widehat{\Psi}_n}\Big(\frac{\widehat{\Psi}_{\lambda r_e}}{\widehat{\Psi}_n}\Big)^2 - \frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{\lambda r_{e-n}}}{\widehat{\Psi}_n}\Big(\frac{\widehat{\Psi}_{(k-1)\lambda r_{e+n}}}{\widehat{\Psi}-n}\Big)^2.$$

L'hypothèse $p \neq 2$ et $r_e \nmid n$ nous donne

$$\frac{\widehat{\Psi}_{k\lambda r_{e+n}}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{(k-2)\lambda r_{e+n}}}{\widehat{\Psi}_n} \equiv \frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n}\Big(\frac{\widehat{\Psi}_{\lambda r_e}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{\lambda r_{e-n}}}{\widehat{\Psi}_n}\Big)\Big(\frac{\widehat{\Psi}_{(k-1)\lambda r_{e+n}}}{\widehat{\Psi}_n}\Big)^2 \pmod{p^{3(e-\nu_p(\widehat{\Psi}_n))}}$$

d'où, puisque $\widehat{\Psi}_{(k-2)\lambda r_{e+n}}/\Psi_n$ est une unité (cf. théorème B)

$$\frac{\widehat{\Psi}_{k\lambda r_{e+n}}}{\widehat{\Psi}_n} \equiv \Big(-\frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{\lambda r_{e-n}}}{\widehat{\Psi}_n}\Big)\Big(\frac{\widehat{\Psi}_{(k-1)\lambda r_{e+n}}}{\widehat{\Psi}_n}\Big)^2\Big/\frac{\widehat{\Psi}_{(k-2)\lambda r_{e+n}}}{\widehat{\Psi}_n} \pmod{p^{3(e-\nu_p(\widehat{\Psi}_n))}}$$

et on termine la démonstration par récurrence sur k. □

En faisant $k = 2$ dans les deux dernières relations contenues dans le lemme 5, nous obtenons le résultat suivant.

COROLLAIRE 1. — *Si r_e ne divise pas n, alors, pour tout $\lambda \in \mathbb{Z}$, on a :*

$$-\frac{\widehat{\Psi}_{\lambda r_{e-n}}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{\lambda r_{e+n}}}{\widehat{\Psi}_n} \equiv -\widehat{\Psi}_{\lambda r_{e-1}}\widehat{\Psi}_{\lambda r_{e+1}} \pmod{p^{2(e-\nu_p(\widehat{\Psi}_n))}}.$$

Comme conséquence du lemme 5 nous obtenons l'énoncé suivant.

LEMME 6. — *Soit r l'ordre d'apparition de p et r_e celui de p^e dans la suite $(\widehat{\Psi}_m)$. Soit $e_0 = \nu_p(\widehat{\Psi}_r)$. On conserve des définitions de a_e, a_{e+1} données dans le théorème C. Alors on a pour $e \geq e_0$*

$$a_{e+1} \equiv a_e^p \pmod{p^{e+1}}, \quad b_{e+1} \equiv b_e^{p^2} \pmod{p^{e+1}}.$$

Preuve. — En utilisant le lemme 5, on a :

$$\begin{aligned} a_{e+1} &= \widehat{\Psi}_{pr_{e+2}}/\widehat{\Psi}_2\widehat{\Psi}_{pr_{e+1}} \\ &\equiv (-\widehat{\Psi}_{r_{e-1}}\widehat{\Psi}_{r_{e+1}})^{\frac{1}{2}p(p-1)}\widehat{\Psi}^p_{r_{e+2}}\widehat{\Psi}_2^{1-p} \\ &\qquad /\widehat{\Psi}_2(-\widehat{\Psi}_{r_{e-1}})^{\frac{1}{2}p(p-1)}(\widehat{\Psi}_{r_{e+1}})^{\frac{1}{2}p(p+1)} \pmod{p^{2e}} \\ &\equiv \widehat{\Psi}^p_{r_{e+2}}\widehat{\Psi}^p_2\widehat{\Psi}^p_{r_{e+1}} \pmod{p^{2e}} \\ &\equiv a_e^p \pmod{p^{e+1}}. \end{aligned}$$

De même, pour b_{e+1}, on a :

$$\begin{aligned} b_{e+1} &= \widehat{\Psi}^2_{pr_{e+1}}\widehat{\Psi}_2/\widehat{\Psi}_{pr_{e+2}} \\ &\equiv (-\widehat{\Psi}_{r_{e-1}}\widehat{\Psi}_{r_{e+1}})^{\frac{1}{2}p(p-1)}(\widehat{\Psi}^2_{r_{e+1}}\widehat{\Psi}_2/\widehat{\Psi}^2_{r_{e+2}})^p \pmod{p^{2e}}. \end{aligned}$$

De plus, d'après le théorème C, on a :

$$-\widehat{\Psi}_{r_{e-1}}\widehat{\Psi}_{r_{e+1}} \equiv -a_e^{-1}b_e\widehat{\Psi}_{-1}\cdot a_eb_e\widehat{\Psi}_1 \equiv b_e^2 \pmod{p^e}.$$

Élevant à la puissance p, on en déduit que :

$$(-\widehat{\Psi}_{r_{e-1}}\widehat{\Psi}_{r_{e+1}})^p \equiv b_e^{2p} \pmod{p^{e+1}}.$$

D'autre part, on a $\widehat{\Psi}^2_{r_{e+1}}\widehat{\Psi}_2/\widehat{\Psi}_{r_{e+2}} = b_e$. Puisque p est supposé impair, on a donc :

$$b_{e+1} \equiv (b_e^{2p})^{\frac{1}{2}(p-1)}b_e^p \equiv b_e^{p^2} \pmod{p^{e+1}}. \qquad \square$$

LEMME 7. — *(On conserve les notations du lemme précédent.) Soit k_e le nombre défini dans le théorème D (i.e. $k_e = \pi_e/r_e$). On a :*

1) si $e_0 > 1$, alors pour tout e tel que $1 < e \leq e_0$, on a $k_e = k_{e-1}$ ou $k_e = pk_{e-1}$

2) si $e_0 \geq 1$, alors pour tout $e \geq e_0$, on a $\theta_{e+1}(a_{e+1}) = \theta_e(a_e)$ et $\theta_{e+1}(b_{e+1}) = \theta_e(b_e^p) = \theta_e(b_e)$ ou $\theta_e(b_e)/p$.

Preuve. — Supposons que $e_0 > 0$ et soit $1 < e \leq e_0$. On veut comparer k_e et k_{e-1}. On a $a_1 = \cdots = a_e = \cdots = a_{e_0}$ et $b_1 = \cdots = b_e = \cdots = b_{e_0}$. Il est clair que $\theta_e(a_e) = \theta_{e-1}(a_{e-1})$ ou $\theta_e(a_e) = p\theta_{e-1}(a_{e-1})$. On a le même énoncé avec b_e, b_{e-1}.

On doit considérer les quatre cas suivants :

$$\text{(i)} \begin{cases} \theta_e(a_e) = \theta_{e-1}(a_{e-1}), \\ \theta_e(b_e) = \theta_{e-1}(b_{e-1})\,; \end{cases} \qquad \text{(ii)} \begin{cases} \theta_e(a_e) = \theta_{e-1}(a_{e-1}), \\ \theta_e(b_e) = p\theta_{e-1}(b_{e-1})\,; \end{cases}$$

$$\text{(iii)} \begin{cases} \theta_e(a_e) = p\theta_{e-1}(a_{e-1}), \\ \theta_e(b_e) = \theta_{e-1}(b_{e-1})\,; \end{cases} \qquad \text{(iv)} \begin{cases} \theta_e(a_e) = p\theta_{e-1}(a_{e-1}), \\ \theta_e(b_e) = p\theta_{e-1}(b_{e-1}). \end{cases}$$

Nous avons vu précédemment (théorème D) que, pour tout $i \geq 1$, on a $k_i = \theta_i(a_i)$ ou $k_i = 2\theta_i(a_i)$.

(a) Si $k_{e-1} = \theta_{e-1}(a_{e-1})$, posons $k_{e-1} = p^h 2^\ell u$ et $\theta_{e-1}(b_{e-1}) = p^{h'} 2^{\ell'} u'$ avec $h' \leq h$, $\ell' \leq \ell$ et $u' \mid u$. Dans les cas (i), (ii) on a $\theta_e(a_e) = k_e = k_{e-1}$. Dans les cas (iii), (iv) on a $\theta_e(a_e) = k_e = pk_{e-1}$.

(b) Si $k_{e-1} = 2\theta_{e-1}(a_{e-1})$ posons $k_{e-1} = 2p^h u$ avec u impair, $\theta_{e-1}(b_{e-1}) = 2p^{h'} u'$ avec $h' \leq h$ et $u' \mid u$. Dans les cas (i), (ii) on a $k_e = 2\theta_e(a_e) = k_{e-1}$. Dans les cas (iii), (iv) on a $k_e = 2\theta_e(a_e) = pk_{e-1}$.

2) Soient $e \geq e_0$, $h_e = \theta_e(a_e) = cp^h$ avec $c \mid p-1$ et $h \leq e-1$. Soit ξ un générateur de $(\mathbb{Z}/p^{e+1}\mathbb{Z})^*$. Alors :

$$a_e \equiv \xi^{\frac{\lambda(p-1)}{c} p^{e-1-h}} \pmod{p^e} \quad \text{avec } (\lambda, h_e) = 1.$$

Donc :

$$a_e \equiv \xi^{\frac{\lambda(p-1)}{c} p^{e-1-h} + \mu(p-1)p^{e-1}} \pmod{p^{e+1}} \quad \text{avec } \mu = 0, 1, \cdots, p-1.$$

Maintenant, le lemme 6 montre que

$$a_{e+1} \equiv a_e^p \equiv \xi^{\frac{\lambda(p-1)}{c} p^{e}-h + \mu(p-1)p^{e}} \equiv \xi^{\frac{\lambda(p-1)}{c} p^{e}-h} \pmod{p^{e+1}},$$

d'où $\theta_{e+1}(a_{e+1}) = cp^h = \theta_e(a_e)$.

Le raisonnement fait ci-dessus est encore valable si on remplace dans les énoncés a_{e+1} par b_{e+1} et a_e par b_e^p car $b_{e+1} \equiv (b_e^p)^p \pmod{p^{e+1}}$. On conclut donc que :

$$\theta_{e+1}(b_{e+1}) = \theta_e(b_e^p) = \theta_e(b_e) \text{ ou } \theta_e(b_e)/p.$$

Cette relation entre $\theta_{e+1}(b_{e+1})$ et $\theta_e(b_e)$ montre qu'au-delà d'un certain rang, b_e est une racine $(p-1)$-ième de l'unité dans $\mathbb{Z}/p^e\mathbb{Z}$.

Nous sommes maintenant en mesure de démontrer le théorème E qui représente le résultat fondamental de ce travail.

Preuve du théorème E.

Soient $e_0 = \nu_p(\widehat{\Psi}_r)$, $a_1 = \widehat{\Psi}_{r+2}/\widehat{\Psi}_2\widehat{\Psi}_{r+1} = \cdots = a_{e_0}$. Soit $\theta_1 = \theta_1(a_1)$.

• Si $e_0 > 1$, soient $e_2 = \nu_p(a_1^{\theta_1} - 1)$ et $e_1 = \inf(e_0, e_2)$. On a $\theta_1(a_1) = \cdots = \theta_{e_1}(a_1) = \theta_1$. On sait que $k_e = \theta_e(a_e)$ ou $k_e = 2\theta_e(a_e)$ (théorème D). Le lemme 7 (1) montre que $k_1 = \cdots = k_{e_1}$ donc $\pi_1 = \cdots = \pi_{e_1}$. Si de plus $e_1 = e_2 < e_0$, le lemme 7 (1) joint au lemme 4 montre que $k_{e_1+1} = pk_{e_1}, \ldots, k_{e_0} = pk_{e_0-1}$ donc $\pi_{e_1+1} = p\pi_{e_1}, \ldots, \pi_{e_0} = p\pi_{e_0-1}$.

• Supposons maintenant que $e \geq e_0$ et montrons que $k_{e+1} = k_e$, ce qui impliquera $\pi_{e+1} = p\pi_e$ puisque $\pi_{e+1} = k_{e+1}r_{e+1} = k_e(pr_e) = p(k_er_e) = p\pi_e$. Le lemme 7 (2) montre que $\theta_{e+1}(a_{e+1}) = \theta_e(a_e)$ et $\theta_{e+1}(b_{e+1}) = \theta_e(b_e)$ ou $\theta_{e+1}(b_{e+1}) = \theta_e(b_e)/p$. On distingue différents cas en tenant compte de la relation $k_i = \theta_i(a_i)$ ou $k_i = 2\theta_i(a_i)$ valable aussi bien pour $i = e$ que pour $i = e + 1$.

(a) $k_e = \theta_e(a_e)$ et $\theta_{e+1}(b_{e+1}) = \theta_e(b_e)$. Dans ce cas $\theta_{e+1}(b_{e+1})$ divise $\theta_{e+1}(a_{e+1})$, donc $k_{e+1} = k_e$.

(b) $k_e = 2\theta_e(a_e)$ et $\theta_{e+1}(b_{e+1}) = \theta_e(b_e)$. Dans ce cas $\theta_e(b_e)$ ne divise pas $\theta_e(a_e)$. On a $\theta_{e+1}(b_{e+1}) = \theta_e(b_e) \mid 2\theta_e(a_e) = 2\theta_{e+1}(a_{e+1})$. De plus $\theta_{e+1}(b_{e+1})$ ne divise pas $\theta_{e+1}(a_{e+1})$, donc $k_{e+1} = 2\theta_{e+1}(a_{e+1}) = k_e$.

(c) $k_e = \theta_e(a_e)$ et $\theta_{e+1}(b_{e+1}) = \theta_e(b_e)/p$. Alors $\theta_e(b_e)/p = \theta_{e+1}(b_{e+1})$ divise $2\theta_{e+1}(a_{e+1}) = 2\theta_e(a_e)$. Comme $\theta_e(b_e)$ divise $\theta_e(a_e)$, on a $\theta_e(b_e)/p \mid \theta_e(a_e)$, d'où $\theta_{e+1}(b_{e+1})$ divise $\theta_{e+1}(a_{e+1})$ et $k_{e+1} = k_e$.

(d) $k_e = 2\theta_e(a_e)$ et $\theta_{e+1}(b_{e+1}) = \theta_e(b_e)/p$. Alors $\theta_e(b_e)/p = \theta_{e+1}(b_{e+1})$ divise $2\theta_{e+1}(a_{e+1}) = 2\theta_e(a_e)$. De plus $\theta_e(b_e)/p$ ne divise pas $\theta_e(a_e)$. Donc $\theta_e(b_e)/p$ ne divise pas $\theta_{e+1}(a_{e+1})$, d'où $k_{e+1} = 2\theta_{e+1}(a_{e+1}) = 2\theta_e(a_e) = k_e$.

6. Points S-entiers sur les courbes elliptiques.

Preuve du théorème F .

1) On a $\pi_1 = p$ et $\nu_p(\widehat{\Psi}_p) = 1$. D'après le théorème E, on a donc $\Pi_N = p^N$ pour tout entier $N \geq 1$.

2) L'affirmation (2.4) est vérifiée pour $N = 2$ par hypothèse. Supposons que (2.4) est vraie au rang $N - 1$ avec $N \geq 3$, c'est-à-dire :

$$\widehat{\Psi}_{p^{N-2}-1}\widehat{\Psi}_{p^{N-2}+1} \equiv -1 \pmod{p^{N-1}}.$$

En utilisant le lemme 5 avec $k = p$, $\lambda = 1$ et $e = N-2$, on obtient

$$\widehat{\Psi}_{p^{N-1}+1} \equiv (-\widehat{\Psi}_{p^{N-2}-1})^{p(p-1)/2}(\widehat{\Psi}_{p^{N-2}+1})^{p(p+1)/2} \pmod{p^{3(N-2)}},$$

$$\widehat{\Psi}_{p^{N-1}-1} \equiv -(-\widehat{\Psi}_{p^{N-2}-1})^{p(p+1)/2}(\widehat{\Psi}_{p^{N-2}+1})^{p(p-1)/2} \pmod{p^{3(N-2)}}$$

d'où :

$$-\widehat{\Psi}_{p^{N-1}-1}\widehat{\Psi}_{p^{N-1}+1} \equiv (-\widehat{\Psi}_{p^{N-2}-1}\widehat{\Psi}_{p^{N-2}+1})^{p^2} \pmod{p^{3(N-2)}}.$$

Or $3(N-2) - N = 2(N-3) \geq 0$, donc :

$$(-\widehat{\Psi}_{p^{N-1}-1}\widehat{\Psi}_{p^{N-1}+1}) \equiv (-\widehat{\Psi}_{p^{N-2}-1}\widehat{\Psi}_{p^{N-2}+1})^{p^2} \pmod{p^N}.$$

Maintenant l'hypothèse de récurrence nous donne :

$$-\widehat{\Psi}_{p^{N-1}-1}\widehat{\Psi}_{p^{N-1}+1} \equiv 1 \pmod{p^N}.$$

3) En tenant compte de la périodicité $(\bmod\ p^N)$ de $(\widehat{\Psi}_m)$ prouvée dans 1), on voit qu'il est équivalent de montrer la proposition suivante : pour tout entier $N \geq 1$ et pour tous entiers m et n premiers à p, on a $\widehat{\Psi}_m \equiv \widehat{\Psi}_n \pmod{p^N} \Rightarrow m \equiv n \pmod{p^N}$.

Supposons que 3) n'est pas vérifiée et soit N_0 le plus petit entier > 0 tel que 3) n'est pas vérifiée, c'est-à-dire il existe $m, n \in \mathbb{Z}$, premiers à p tels que $m \not\equiv n \pmod{p^{N_0}}$ et $\widehat{\Psi}_m \equiv \widehat{\Psi}_n \pmod{p^{N_0}}$. En vertu de l'hypothèse faite sur les classes $(\bmod\ p^2)$, on peut supposer que $N_0 \geq 3$.

On a $\widehat{\Psi}_m = \widehat{\Psi}_n \pmod{p^{N_0-1}}$, donc $m = n \pmod{p^{N_0-1}}$. Posons $m = n + \lambda p^{N_0-1}$, $(\lambda, p) = 1$, $\lambda = kp \pm \ell = \ell = 1, \cdots, (p-1)/2$. On a :

$$\widehat{\Psi}_m \equiv \widehat{\Psi}_n \equiv \widehat{\Psi}_{n+(kp\pm\ell)p^{N_0-1}} \equiv \widehat{\Psi}_{n\pm\ell p^{N_0-1}} \pmod{p^{n_0}}.$$

On en déduit que $\widehat{\Psi}_{\ell_{p^{N_0-1}+n}} \equiv \widehat{\Psi}_n$ ou $\widehat{\Psi}_{\ell_{p^{N_0-1}-n}} \equiv \widehat{\Psi}_{-n} \pmod{p^{N_0}}$. Quitte à remplacer n par $-n$, on peut supposer qu'on a le premier cas, c'est-à-dire $\widehat{\Psi}_{\ell_{p^{N_0-1}+n}} \equiv \widehat{\Psi}_n \pmod{p^{N_0}}$. Comme $r = p$ ne divise pas n, on a $\widehat{\Psi}_{\ell_{p^{N_0-1}+n}}/\widehat{\Psi}_n \equiv 1 \pmod{p^{N_0}}$. En appliquant la quatrième formule contenue dans le lemme 5 avec $k = p$, $\lambda = \ell$ et $r_e = p^{N_0-2}$, on obtient modulo $p^{3(N_0-2)}$:

$$\frac{\widehat{\Psi}_{\ell_{p^{N_0-1}+n}}}{\widehat{\Psi}_n} = \frac{\widehat{\Psi}_{p(\ell p^{N_0-2})+n}}{\widehat{\Psi}_n}$$
$$\equiv \Big(-\frac{\widehat{\Psi}_{\ell_{p^{N_0-2}+n}}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{\ell_{p^{N_0-2}-n}}}{\widehat{\Psi}_n}\Big)^{\frac{1}{2}p(p-1)}\Big(\frac{\widehat{\Psi}_{\ell_{p^{N_0-2}+n}}}{\widehat{\Psi}_n}\Big)^p.$$

Cette congruence est valable $(\bmod p^{N_0})$ car $3(N_0-2)-N_0 \geq 0$.

L'application de ce même lemme avec $k=\ell$, $\lambda=1$ et $r_e=p^{N_0-2}$ nous donne modulo $p^{3(N_0-2)}$:

$$\frac{\widehat{\Psi}_{\ell_{p^{N_0-2}+n}}}{\widehat{\Psi}_n} \equiv \Big(-\frac{\widehat{\Psi}_{p^{N_0-2}-n}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{p^{N_0-2}+n}}{\widehat{\Psi}_n}\Big)^{\frac{1}{2}\ell(\ell-1)}\Big(\frac{\widehat{\Psi}_{p^{N_0-2}+n}}{\widehat{\Psi}_n}\Big)^{\ell},$$
$$\frac{\widehat{\Psi}_{p^{N_0-2}-n}}{\widehat{\Psi}_n} \equiv \Big(-\frac{\widehat{\Psi}_{p^{N_0-2}-n}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{p^{N_0-2}+n}}{\widehat{\Psi}_n}\Big)^{\frac{1}{2}\ell(\ell-1)}\Big(-\frac{\widehat{\Psi}_{p^{N_0-2}-n}}{\widehat{\Psi}_n}\Big)^{\ell}.$$

On en déduit que :

$$\begin{aligned}
&\frac{\widehat{\Psi}_{\ell_{p^{N_0-2}+n}}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{\ell_{p^{N_0-2}-n}}}{\widehat{\Psi}_n}\\
&\quad\equiv \Big(-\frac{\widehat{\Psi}_{p^{N_0-2}-n}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{p^{N_0-2}+n}}{\widehat{\Psi}_n}\Big)^{\ell(\ell-1)}\Big(-\frac{\widehat{\Psi}_{p^{N_0-2}-n}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{p^{N_0-2}+n}}{\widehat{\Psi}_n}\Big)^{\ell}\\
&\quad\equiv \Big(-\frac{\widehat{\Psi}_{p^{N_0-2}-n}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{p^{N_0-2}+n}}{\widehat{\Psi}_n}\Big)^{\ell^2} \bmod p^{3(N_0-2)}.
\end{aligned}$$

Ces congruences restent valables $(\bmod p^{N_0})$. Revenons au calcul de $\widehat{\Psi}_{p^{N_0-1}+n}/\Psi_n$. Nous obtenons :

$$\frac{\widehat{\Psi}_{\ell_{p^{N_0-1}+n}}}{\widehat{\Psi}_n} \equiv \Big(-\frac{\widehat{\Psi}_{p^{N_0-2}-n}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{p^{N_0-2}+n}}{\widehat{\Psi}_n}\Big)^{\frac{1}{2}\ell^2 p(p-1)}\Big(\frac{\widehat{\Psi}_{\ell_{p^{N_0-2}+n}}}{\widehat{\Psi}_n}\Big) \ (\bmod p^{N_0}).$$

Comme r ne divise pas n, d'après le corollaire 1 ci-dessus avec $\lambda=1$ et $r_e=p^{N_0-2}$, on a :

$$-\frac{\widehat{\Psi}_{p^{N_0-2}-n}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{p^{N_0-2}+n}}{\widehat{\Psi}_n} \equiv -\widehat{\Psi}_{p^{N_0-2}-n}\widehat{\Psi}_{p^{N_0-2}+n} \ (\bmod p^{2(N_0-2)}).$$

Par suite, comme $2(N_0-2)\geq N_0-1$, on déduit de la relation

$$-\widehat{\Psi}_{p^{N_0-2}-1}\widehat{\Psi}_{p^{N_0-2}+1} \equiv 1 \ (\bmod p^{N_0-1})$$

prouvée dans 2), identité (2.4), la congruence :

$$-\frac{\widehat{\Psi}_{p^{N_0-2}-n}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{p^{N_0-2}+n}}{\widehat{\Psi}_n} \equiv 1 \ (\bmod p^{N_0-1}).$$

Alors il vient :

$$\Big(-\frac{\widehat{\Psi}_{p^{N_0-2}-n}}{\widehat{\Psi}_n}\frac{\widehat{\Psi}_{p^{N_0-2}+n}}{\widehat{\Psi}_n}\Big)^p \equiv 1 \pmod{p^{N_0}}.$$

D'où, puisque $(p-1)$ est pair :

$$\frac{\widehat{\Psi}_{\ell_{p^{N_0-1}+n}}}{\widehat{\Psi}_n} \equiv \Big(\frac{\widehat{\Psi}_{\ell_{p^{N_0-2}+n}}}{\widehat{\Psi}_n}\Big)^p \equiv 1 \pmod{p_0^N}.$$

Posons $X = (\widehat{\Psi}_{\ell p^{N_0-2}+n})/\widehat{\Psi}_n$. On a $X^p - 1 \equiv 0 \pmod{p^{N_0}}$. De plus $X \equiv 1 \pmod{p^{N_0-2}}$, car p^{N_0-2} est une période de $(\widehat{\Psi}_m)$ modulo p^{N_0-2}. Comme $(X-1)(X^{p-1}+X^{p-2}+\cdots+X+1) = 0 \pmod{p^{N_0}}$ et $X^{p-1}+X^{p-2}+\cdots+X+1 = p \pmod{p^2}$, on a $X \equiv 1 \pmod{p^{N_0-1}}$, c'est-à-dire $\Psi_{\ell p^{N_0-2}+n} \equiv \widehat{\Psi}_n \pmod{p^{N_0-1}}$, ce qui contredit le caractère minimal de N_0.

4) Supposons que $\widehat{\Psi}_m = \pm 1$. Quitte à remplacer m par $-m$, on peut supposer que $m > 0$. On a $(m,p) = 1$ car p divise $\widehat{\Psi}_p$. Pour tout entier $N \geq 1$, on fait la division euclidienne de m par p^N. On obtient $m = p^N k + t_N$ avec $1 \leq t_N \leq p^{N-1}$ et $(t_N, p) = 1$. On a $\pm 1 = \widehat{\Psi}_m \equiv \widehat{\Psi}_{t_N} \pmod{p^N}$.

- Si on a le signe '+', on obtient $1 = \widehat{\Psi}_1 \equiv \widehat{\Psi}_{t_N} \pmod{p^N}$. D'après 3), on a donc $t_N = 1$ pour tout $N \geq 1$, d'où $m = 1$.

- Si on a le signe '−', on obtient $-1 \equiv \widehat{\Psi}_{p^{N}-1} \equiv \widehat{\Psi}_{t_N} \pmod{p^N}$, d'où $t_N = p^{N-1} - 1$ pour tout $N \geq 1$ d'après 3). On en déduit que, pour tout $N \geq 1$, on a $m = p^N k + p^N - 1$, ce qui donne $m = -1$.

Finalement, on obtient $m = \pm 1$. L'implication réciproque est évidente puisque $\widehat{\Psi}_1 = 1$ et $\widehat{\Psi}_{-1} = -1$, ce qui achève la démonstration du théorème F.

Nous allons maintenant donner quelques exemples d'application de ce théorème F.

a) *Multiples S-entiers de $M = (1/5^2, (1+k5^4)/5^3)$ sur la courbe $y^2 = x^3 + 2kx + 25k^2$ avec k entier $\neq 0$ et $(k,5) = 1$.*

Le lemme A montre que 5 divise le dénominateur de mM pour tout entier $m \neq 0$. Considérons les multiples de M qui sont S-entiers avec $S = \{5\}$. On a le résultat suivant :

THÉORÈME 2. — *Soient $M = (1/5^2, (1+k5^4)/5^3)$ avec k entier $\neq 0$ non divisible par 5. Soit $S = \{5\}$. Alors les multiples S-entiers de M sur la courbe $y^2 = x^3 + 2kx + 25k^2$ sont $\pm M$.*

Preuve. — On applique le théorème F avec $p = 5$. On pose $\widehat{\Psi}_m = 5^{m^2-1}\Psi_m(M)$. On a :

$$\begin{aligned}
\widehat{\Psi}_2 &= 2(1 + k5^4) \equiv 2 \pmod{5^4},\\
\widehat{\Psi}_3 &= 3 + 12k5^4 + 8k^2 5^8 \equiv 3 \pmod{5^4},\\
\widehat{\Psi}_4 &= 4(1 + k5^4)(1 + 2k5^5 - 16k^3 5^{12} - 8k^4 5^1 6) \equiv 4 \pmod{5^4}.
\end{aligned}$$

On en déduit, par récurrence sur m, que $\widehat{\Psi}_m = m \pmod{5^4}$. Puisque ici $d = 5$, le point $M \pmod 5$ est non singulier, $r = r(5) = 5$ et $\nu_p(\widehat{\Psi}_5) = 1$ d'après le lemme 1. De plus on a :

$$\widehat{\Psi}_{5-1}\widehat{\Psi}_{5+1} = \widehat{\Psi}_4\widehat{\Psi}_6 \equiv 24 \pmod{5^4} \equiv -1 \pmod{5^2}.$$

Puisque $\widehat{\Psi}_m = m \pmod{5^4}$, alors les éléments $\widehat{\Psi}_m$, $1 \leq m \leq 5^3 - 1$ sont distincts deux à deux $(\mathrm{mod}\ 5^3)$, de sorte que les hypothèses du théorème F sont vérifiées. On en déduit que $\widehat{\Psi}_m = \pm 1$ implique $m = \pm 1$.

Supposons maintenant que mM est S-entier et posons $m = 5^e m'$, avec $e \geq 0$ et $(5, m') = 1$. Si $e \geq 1$, alors $5M$ est S-entier. En tenant compte de $\nu_p(\widehat{\Psi}_5) = 1$ et en utilisant le corollaire A, nous obtenons $\widehat{\Psi}_5 = \pm 5$. Quelques calculs $(\mathrm{mod}\ 5^5)$ donnent :

$$\begin{aligned}
\widehat{\Psi}_2 &= 2(1 + k5^4),\\
\widehat{\Psi}_3 &\equiv 3(1 + 4k5^4),\\
\widehat{\Psi}_4 &\equiv 4(1 + k5^4),\\
\widehat{\Psi}_5 &= \widehat{\Psi}_4\widehat{\Psi}_2^3 - \widehat{\Psi}_3^3 \equiv 5 - 196k5^4 \pmod{5^5} \not\equiv \pm 5 \pmod{5^5}.
\end{aligned}$$

On en déduit que $e = 0$, $m = m'$ et $\widehat{\Psi}_m = \pm 1$, d'où $m = \pm 1$ en vertu du théorème F.

b) *Points S-entiers sur la courbe $y^2 = x^3 - 13$.*

Cette courbe est de rang 1 sur $\mathbb{Q}$, sans torsion et son groupe des points rationnels est engendré par $M = (17, 70)$ (cf. [4]). Le théorème F s'applique à cette courbe et à ce point pour $p = 3$. Pour tout nombre premier ℓ, le point $M \pmod{\ell}$ est non singulier. On a ici $d = 1$ et $\widehat{\Psi}_m = \Psi_m(M)$.

Quelques calculs modulo 27 nous donnent :

$$\begin{array}{llllll}\widehat{\Psi}_0=0, & \widehat{\Psi}_1\equiv 1, & \widehat{\Psi}_2\equiv 5, & \widehat{\Psi}_3\equiv -3, & \widehat{\Psi}_4\equiv -2, & \widehat{\Psi}_5\equiv -7,\\ \widehat{\Psi}_6\equiv -6, & \widehat{\Psi}_7\equiv 13, & \widehat{\Psi}_8\equiv -10, & \widehat{\Psi}_9\equiv -9 & \widehat{\Psi}_{10}=-8, & \widehat{\Psi}_{11}\equiv -4,\\ \widehat{\Psi}_{12}\equiv -12, & \widehat{\Psi}_{13}\equiv -11, & \widehat{\Psi}_{14}\equiv 11, & \widehat{\Psi}_{15}\equiv 12, & \widehat{\Psi}_{16}\equiv 4, & \widehat{\Psi}_{17}\equiv 8,\\ \widehat{\Psi}_{18}\equiv 9, & \widehat{\Psi}_{19}=10, & \widehat{\Psi}_{20}=-13, & \widehat{\Psi}_{21}\equiv 6, & \widehat{\Psi}_{22}\equiv 7, & \widehat{\Psi}_{23}\equiv 2,\\ \widehat{\Psi}_{24}\equiv 3, & \widehat{\Psi}_{25}\equiv -5, & \widehat{\Psi}_{26}\equiv -1 & \pmod{27}. & & \end{array}$$

Cela montre que les éléments Ψ_m pour $1\le m\le 26$ et $(m,3)=1$ sont distincts deux à deux (mod 27), et on a $\nu_3(\widehat{\Psi}_3)=1$ et $\widehat{\Psi}_{3-1}\widehat{\Psi}_{3+1}=\widehat{\Psi}_2\widehat{\Psi}_4\equiv -1 \pmod 9$, ce qui vérifie les conditions du théorème F. On en déduit que $\widehat{\Psi}_m=\pm 1$ implique $m=\pm 1$. On a alors le résultat suivant.

THÉORÈME 3. — *Soient $S=\{2,3,5,7\}$ et $M=(17,70)$. Les points S-entiers sur la courbe $y^2=x^3-13$ sont :*

$$\pm M=(17,\pm 70),\quad \pm 2M=\Big(\frac{85289}{2^4\cdot 5^2\cdot 7^2},\pm\frac{22858837}{2^6\cdot 5^3\cdot 7^3}\Big).$$

Preuve. — On a $\widehat{\Psi}_2=2^2\cdot 5\cdot 7$, ce qui montre que M est d'ordre 2 dans les groupes $E(\mathbb{F}_2)_{n\cdot s}$, $E(\mathbb{F}_5)$ et $E(\mathbb{F}_7)$. Donc $\widehat{\Psi}_m\equiv 0 \pmod 2$ (resp. mod 5, mod 7) si et seulement si $m\equiv 0 \pmod 2$. De même $\widehat{\Psi}_m\equiv 0$ (mod 3) si et seulement si $m\equiv 0 \pmod 3$.

Soit m un entier rationnel non nul. Supposons que mM est S-entier et posons $m=2^{h_1}3^{h_2}m'$ avec $(m',6)=1$. Si $h_1\ge 1$, alors $2M,\dots,2^{h_1}M$ sont S-entiers d'après le lemme A. Le point $2M$ est effectivement S-entier puisque $\widehat{\Psi}_2=2^2{\cdot}5{\cdot}7$. Le point $4M$ ne l'est pas puisque $\widehat{\Psi}_4=2^3{\cdot}5{\cdot}7{\cdot}22858837$ d'où $h_1=0$ ou $h_1=1$. On a $\widehat{\Psi}_3=3\cdot 17\cdot 4861$, donc $3M$ n'est pas S-entier et $h_2=0$. L'application du lemme A montre que $m'M$ est S-entier donc $\widehat{\Psi}_{m'}=\pm 1$, d'où $m'=\pm 1$ d'après le théorème F et par suite $m=\pm 1$, ± 2.

c) *Points S-entiers sur la courbe $y^2=x^3+40$.*

Cette courbe est de rang 1 sur Q, sans torsion (cf. [4]). Son groupe des points rationnels est engendré par $M=(6,16)$. Cette courbe a mauvaise réduction en $2,3,5$ et le point M est singulier (mod 2). D'après le théorème A, 2 divise Ψ_m pour tout entier $m\ne\pm 1$.

Cette courbe a été étudiée dans [1]; certains arguments seront d'ailleurs repris de [1]. La méthode utilisée ici est différente puisque nous faisons usage du théorème F avec $p=5$. Pour tout entier $m\ne 0$, on pose $\Psi_m(6,16)=2^{e(m)}\bar{\Psi}_m$ avec $\bar{\Psi}_m$ impair. On a le :

LEMME 8. — *Les exposants $e(m)$ sont donnés par :*

$$e(m) = \begin{cases} \frac{1}{2}(m^2 - 1) & \text{si } m \text{ est impair,} \\ \frac{1}{2}m^2 + M + 2 & \text{si } m = 2^M n \text{ (avec } M \geq 1 \text{ et } n \text{ impair).} \end{cases}$$

Preuve. — Voir [1].

THÉORÈME 4. — *Soit $S = \{2, 3, 5, 7\}$. Les points S-entiers sur la courbe $y^2 = x^3 + 40$ sont :*

$$\pm M = (6, \pm 16), \quad \pm 2M = \left(-\frac{39}{2^6}, \pm\frac{3229}{2^9}\right).$$

Preuve. — Soit m un entier $\neq 0$. Supposons que mM est S-entier et posons $m = 2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3} \cdot 7^{e_4} m'$ avec $(m', 2 \cdot 3 \cdot 5 \cdot 7 \cdot) = 1$. Le raisonnement fait dans [1] montre que $e_1 = 0$ ou 1, $e_2 = e_3 = e_4 = 0$. L'application du lemme A montre que $m'M$ est S-entier, donc $\widehat{\Psi}_{m'} = (\pm 2)^{\frac{1}{2}(m'^2 - 1)}$ d'après le corollaire A et le lemme 8. L'entier m' étant impair, on a $m' \equiv \pm 1 \pmod 4$. Posons $m' = 4k \pm 1$ et supposons que $k \neq 0$. Puisque $(m', 5) = 1$, on peut rejeter les cas $k \equiv 1$, $m' = 4k + 1$ et $k \equiv -1 \pmod 5$, $m' = 4k - 1$. Reste à considérer les cas suivants :

(i) Si $k \equiv 1 \pmod 5$ et $m' = 4k - 1$. Dans ce cas on a d'une part $m' \equiv 3 \pmod 5$ et d'autre part on a $(m'^2 - 1)/2 \equiv 0 \pmod 4$, d'où $\Psi_{m'} = \pm 2^{\frac{1}{2}(m'^2 - 1)} \equiv \pm 1 \pmod 5$, ce qui contredit le 3) du théorème F.

(ii) Si $k \equiv -1 \pmod 5$ et $m' = 4k + 1$ on arrive aussi à une contradiction puisque $m' \equiv -3 \pmod 5$ et $\widehat{\Psi}_{m'} \equiv \pm 1 \pmod 5$.

(iii) Si $k \equiv 2 \pmod 5$ et $m' = 4k + 1$ on a $(m'^2 - 1)/2 \equiv 0 \pmod{20}$, donc $\Psi_{m'} = \pm 2^{\frac{1}{2}(m'^2 - 1)} \equiv \pm 1 \pmod{5^2}$. D'autre part $k \equiv 2 \pmod 5$ implique $k \equiv 2, 7, -3 \pmod{25}$, donc $m' = 9, 4, -11 \pmod{25}$ et $\Psi_{m'} \not\equiv \pm 1 \pmod{25}$, ce qui contredit le résultat ci-dessus.

(iv) Si $k \equiv 2 \pmod 5$ et $m' = 4k - 1$, on a d'une part $m' \equiv 2 \pmod 5$. D'autre part $(m'^2 - 1)/2 \equiv 0 \pmod 4$ donc $\Psi_{m'} = \pm 2^{\frac{1}{2}(m^2 - 1)} \equiv \pm 1 \pmod 5$, ce qui est contradictoire.

(v) Si $k \equiv -2 \pmod 5$ et $m' = 4k + 1$, on a d'une part $m' \equiv -2 \pmod 5$. D'autre part $(m'^2 - 1)/2 \equiv 0 \pmod 4$ donc $\Psi_{m'} = \pm 2^{\frac{1}{2}(m^2 - 1)} \equiv \pm 1 \pmod 5$, ce qui est contradictoire.

(vi) Si $k \equiv -2 \pmod 5$ et $m' = 4k - 1$, on a $k \equiv -2, -7, 3 \pmod{5^2}$, donc $m' \equiv -9, -4, 11 \pmod{25}$. D'autre part $(m'^2 - 1)/2 \equiv 0 \pmod{20}$ donc $\Psi_{m'} = \pm 2^{\frac{1}{2}(m^2-1)} \equiv \pm 1 \pmod{5^2}$, ce qui est contradictoire.

(vii) Si $k \equiv 0 \pmod 5$ et $m' = 4k \pm 1$. On pose $k = 5^N \lambda \cdot N \geq 1$ avec $(\lambda, 5) = 1$

- Si λ est impair, alors $(m'^2 - 1)/2 \equiv 2 \pmod 4$ donc $\Psi_{m'} = \pm 2^{\frac{1}{2}(m^2-1)}$ $\not\equiv \pm 1 \pmod 5$. D'autre part, $m' \equiv \pm 1 \pmod 5$ donc $\Psi_{m'} \equiv \pm 1 \pmod 5$, ce qui est contradictoire.
- Si λ est pair on pose $k = 5^N \cdot 2^M k'$ et $m' = 5^N 2^{M+2} k' \pm 1$ avec $M \geq 1$ et $(k', 5) = 1$. On a $(m'^2 - 1)/2 \equiv 5^N 2^{M+2}(5^N 2^{M+1} k'^2 \pm k')$ donc $\widehat{\Psi}_{m'} = \pm 2^{\frac{1}{2}(m'^2-1)} \equiv \pm 1 \pmod{5^{N+1}}$, ce qui est contradictoire à $m' \equiv 5^N 2^{M+2} k' \pm 1 \pmod{5^{N+1}}$.

Finalement on obtient $k = 0$, $m' = \pm 1$ et $m = \pm 1, \pm 2$.

7. Quelques questions relatives aux suites elliptiques.

a) Considérons la suite de Fibonacci $F_0 = 0$, $F_1 = 1$ et

$$F_n = F_{n-1} + F_{n-2} \quad \text{pour } n \geq 2.$$

Désignons par $r(p^e)$ l'ordre d'apparition de p^e dans cette suite et par $\pi(p^e)$ la période de cette suite (mod p^e). Dans [10], D.D. Wall pose la question : « a-t-on $\pi(p) \neq \pi(p^2)$ pour tout nombre premier impair ? »

Plusieurs auteurs ont abordé ce problème et cette inégalité a été vérifiée pour tous les nombres premiers p tels que $p < 10^9$ (cf. [14]). En fait pour cette suite particulière on a :

$$r(p) = r(p^2) \Longleftrightarrow \pi(p) = \pi(p^2) \Longleftrightarrow F_{p-\left(\frac{5}{p}\right)} \equiv 0 \pmod{p^2}.$$

Il est prouvé dans [15] que si $\pi(p) \neq \pi(p^2)$, alors le premier cas du théorème de Fermat a lieu pour l'exposant p.

Revenons aux suites elliptiques. L'existence du rang e_1 dans le théorème E montre que si $\pi(p) = \pi(p^2)$, alors $r(p) = r(p^2)$, l'implication réciproque étant fausse.

Question. — Une suite elliptique étant donnée, existe-t-il un nombre premier p tel que $r(p) = r(p^2)$? L'ensemble de tels nombres premiers est-il fini ? Si cet ensemble est non vide, que dire du sous-ensemble formé des nombres premiers tels que $\pi(p) = \pi(p^2)$?

b) Considérons les suites linéaires (U_n) telles que $U_{n+2} = kU_{n+1} + U_n$, avec $k \in \mathbb{Z}$ et $(U_0, U_1) = (0,1)$. Soient p un nombre premier et $\pi(p)$ la période de $(U_n) \pmod p$. Pour tout $\bar{\ell} \in \mathbb{Z}/p\mathbb{Z}$, on définit la fréquence de $\bar{\ell}$ comme étant

$$f(\bar{\ell}, p) = \#\{n \mid 0 \leq n \leq \pi(p) - 1,\ U_n \equiv \ell \pmod p\}.$$

Soit $\mathcal{F}(p)$ l'ensemble des fréquences $(\mathrm{mod}\, p)$ des différentes classes modulo p. A. Schinzel [9] a montré que si $p > 7$ et $p \nmid a(a^2+4)$, on a :

$$\begin{aligned}
\mathcal{F}(p) &= \{0,1,2\} \text{ ou } \{0,1,2,3\} \text{ si } \pi(p) \not\equiv 0 \pmod 4,\\
&= \{0,2,4\} \text{ si } \pi(p) \equiv 4 \pmod 8,\\
&= \{0,1,2\} \text{ ou } \{0,2,3\} \text{ ou } \{0,1,2,4\}\\
&\qquad\qquad \text{ ou } \{0,2,3,4\} \text{ si } \pi(p) \equiv 0 \pmod 8.
\end{aligned}$$

J. Pihko [8] a obtenu un résultat semblable lorsque $(U_0, U_1) = (2, a)$.

Question. — Une suite elliptique étant donnée, on définit comme ci-dessus les fréquences des classes $(\mathrm{mod}\, p)$. A-t-on un énoncé semblable pour une telle suite ?

BIBLIOGRAPHIE

[1] M. AYAD, Points S-entiers des courbes elliptiques, Manuscripta Math., 76 (1992), 305–324.

[2] R.A. BATEMAN, E.A. CLARCK, M. HANCOCK, C.A. REITER, The Period of Convergents modulo M of Reduced Quadratic Irrationals, Fibo. Quarterly, 29 (1991), 220–229.

[3] P.R.D. CARMICHAEL, On Sequences of Integers defined by Recurrence Relations, Quarterly J. of Math., 48 (1920), 343–372.

[4] J.W.S. CASSELS, The Rational Solutions of the Diophantine Equation $y^2 = x^3 - D$, Acta Math., 82 (1950), 243–273.

[5] A.T. ENGSTROM, On Sequences defined by Linear Recurrence Relations, Trans. A.M.S., 33 (1931), 210–218.

[6] M. HALL, An Isomorphism between Linear Recurring Sequences and Algebraic Rings, Trans. Amer. Math. Soc., 44 (1938), 196–218.

[7] E. LUTZ, Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques, J. Reine Angew. Math., 177 (1937), 237–247.

[8] J. PIHKO, A Note on a Theorem of Schinzel, Fibo. Quarterly, 29 (1991), 333–338.

[9] A. SCHINZEL, Special Lucas Sequences, including the Fibonacci Sequence modulo a Prime. In a tribute to Paul Erdos, A. Baker, B. Bollobas and A. Hajnal Ed., Cambridge University Press (1990), 349–357.

[10] D.D. WALL, Fibonacci Series modulo m, Amer. Math. Monthly, 67 (1960), 525–532.

[11] M. WARD, The Characteristic Number of a Sequence of Integers Satisfying a Linear Recursion Relation, Trans. Amer. Math. Soc., 33 (1931), 153–165.

[12] M. WARD, Memoir on Elliptic Divisibility Sequences, Amer. J. of Math., 70 (1948), 31–74.

[13] M. WARD, The Law of Repetition of Primes in an Elliptic Divisibility sequence, Duke Math. J., 15 (1948), 941–946.

[14] H.C. WILLIAMS, A Note on the Fibonacci Quotient $F_{p-\varepsilon}/p$, Canad. Math. Bull., 25 (1982), 366–370.

[15] ZHI-HONG SUN and ZHI-WEI SUN, Fibonacci Numbers and Fermat's Last Theorem, Acta Arith., 60 (1992), 371–388.

Manuscrit reçu le 12 novembre 1992.

Mohamed AYAD,
Université de Caen
Département de Mathématiques
14032 Caen Cedex (France).